# ネットワーク機器における 脆弱性検知の取り組みと課題

中岡 典弘 , 井上 圭 @ JANOG 52

# 発表者紹介

中岡 典弘

- Twitter: @MaineK00n
- Vuls committer

井上 圭

- Twitter: @hogehuga
- セキュリティコンサルタント
- 脆弱性対応支援業務

# ネットワーク機器の脆弱性管理について

# ネットワーク機器とサーバの脆弱性管理の違い

私たちはサーバ系の脆弱性管理を主に行っていますが、ネットワーク機器等の脆弱性管理をする際に以下の点が異なると感じている。

サーバ

- 更新プログラムを基に、**残存する脆弱性**の危険度を優先度付けをして対応を決める

ネットワーク機器

- バージョン管理というより、話題になるほど**危険な脆弱性が出た時**に対応を決める

相当大きな脆弱性が出るまでバージョンアップはせず、それ以外の残存する脆弱性について考慮がされていない。ここがサーバ運用との違いと考える。

これをサーバと同じような脆弱性管理フローに載せることで、よりセキュアに、残存脆弱性を可視化した状態にしたい。

# 想定している対応

現状（一般的な方法と想定）

- 台帳でネットワーク機器情報を管理（ファームウェアバージョン等）
- 重大な脆弱性公開時に、台帳と突合し、対象を洗い出す

単一ベンダであればベンダツールで管理は可能な場合も多いが、複数ベンダの機器を使うと台帳管理になることが多い。
台帳管理では棚卸による最新化が必要だが、頻繁に行うことが難しい。

将来

- 外部から安全な方法で定期スキャンを行い、ネットワーク機器情報を管理
- 重大な脆弱性公開時に、最新の機器情報で突合し、対象を洗い出す

外部からの定期スキャンにより、常に台帳の最新化を行う。
また、統一した方法により、ベンダが異なっても利用可能。
定期スキャンと合わせることで、脆弱性情報をいち早く反映可能。

# どうしたらよいか

ネットワーク機器の脆弱性情報データベースを用意する

- サーバの脆弱性情報同様、NVD にはある

安全なマルチベンダで使えるスキャンを用意する

- SNMP で取得ができる
- （SSH や Telnet もいいが、直接アクセスなので利用したくない）

バージョン情報を脆弱性データベースとマッチングさせせる

- 現状だと NVD の情報と CPE を使う方法が行われやすい

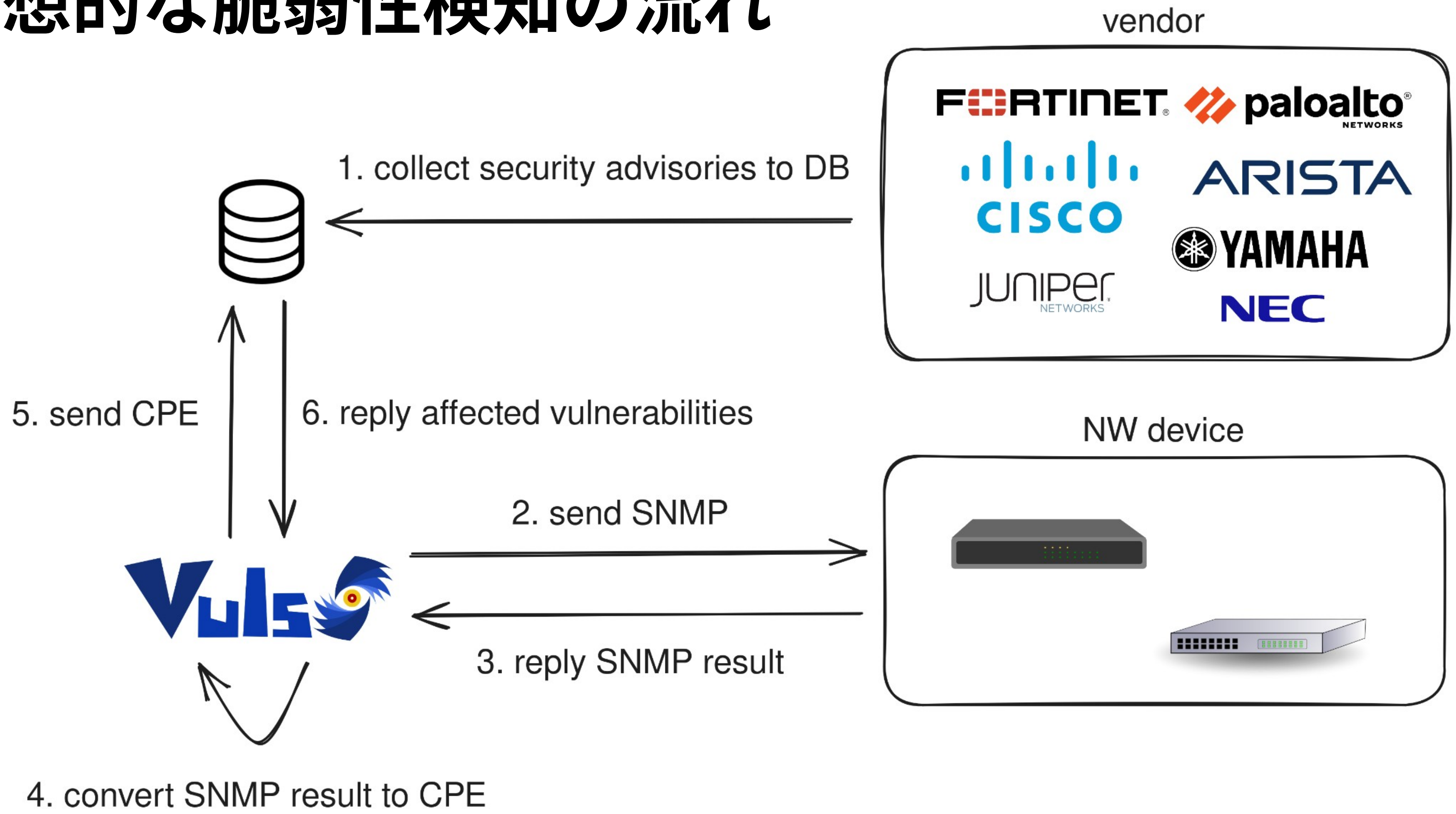
# 今回の議題

本発表では、これらについて確認したことを発表し、ネットワーク機器の脆弱性管理について考えたい

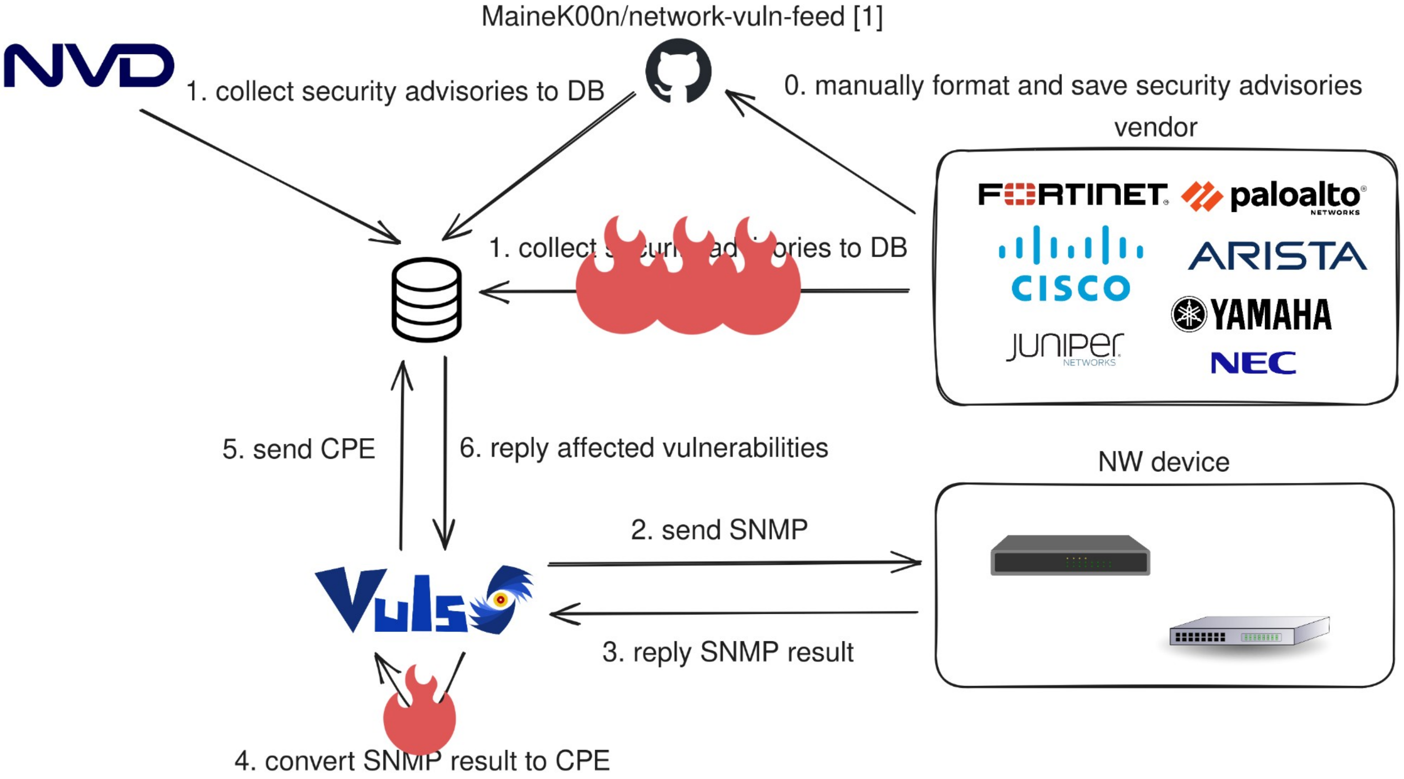
- ネットワーク機器における、脆弱性検知について
- ネットワーク機器の、脆弱性アドバイザリの収集について
- ネットワーク機器の特定について（ SNMP を利用）
- 結論、及びディスカッション

# NW 機器における脆弱性検知（現実）

# 理想的な脆弱性検知の流れ



# 現実はアドバイザリの収集と NW 機器の特定に難あり


MaineK00n/network-vuln-feed [1]
NVD
1. collect security advisories to DB
0. manually format and save security advisories
vendor
FORTINET
paloalto NETWORKS
CISCO
ARISTA
YAMAHA
JUNIPER NETWORKS
NEC
1. collect s curi ad ories to DB
5. send CPE
6. reply affected vulnerabilities
NW device
2. send SNMP
Vuls
3. reply SNMP result
4. convert SNMP result to CPE

[1] https://github.com/MaineK00n/network-vuln-feed

# 脆弱性アドバイザリの収集

# 脆弱性アドバイザリの提供状況

現状、複数の提供元から、複数の形式で提供されている

- Fortinet: CVRF で提供
- Cisco Systems: CVRF/CSAF で提供、 CVRF をリストしているページもあり
- Juniper Networks: HTML のみ？
- Palo Alto Networks: MITRE CVE 4.0 JSON Format で提供
- Arista Network:  一部 CSAF で提供、 HTML/PDF のみの提供もあり
- YAMAHA: HTML のみ？
- NEC: HTML のみ？

# 機械的に収集できない脆弱性アドバイザリあるある①

- NVD の情報を使えば？→ 使えない……
  - 脆弱性アドバイザリの公開から、 NVD で取り込まれるまでに時間がかかるものも
  - 脆弱性アドバイザリと NVD の間で影響するバージョンが異なっているものが複数あり
- エラーでアクセスできない
  - https://www.fortiguard.com/psirt/FG-IR-012-001
- HTML や PDF のみの提供
  - HTML が当時と変わっていて、 HTML から情報を取得することに失敗する場合も
- Web 版と CVRF/CSAF で記述内容が異なる
  - Web 版の更新内容が CVRF/CSAF に反映されていないことも
- 定期的な取得がかなり大変
  - 大量のページネーションが必要なことも

# 機械的に収集できない脆弱性アドバイザリあるある②

- CVRF/CSAF の仕様を満たしていない・適したフィールドを利用しない
    - CVE ID が 1 箇所にまとめて書いてある、 Notes に何でも書いてしまう
- 内容の解釈が難しい……
    - アドバイザリごとに異なるバージョン記述

      6.0.0 to 6.0.4, lower than 3.2.0, 7.3.0 through 7.3.1, 5.4.0 and 5.4.1, …
    - 影響するバージョンはどこからどこまで？
        - 4.2: 4.2.0 or (≧ 4.2.0, ≦ 4.2.x)
        - 5.2.2 and below, 5.0.11 and below: (≦ 5.0.11, ≦ 5.2.2) or (≦ 5.0.11, ≧ 5.2.0, ≦ 5.2.2)
          or (≧ 5.0.0, ≦ 5.0.11, ≧ 5.2.0, ≦ 5.2.2)
    - 存在しないと思われるバージョンを参照している

      FortiExtender 5.3 all versions (ref: https://www.fortiguard.com/psirt/FG-IR-22-048

      FortiExtender 5.3 は存在しない？ (ref: https://docs.fortinet.com/product/fortiextender/5.3

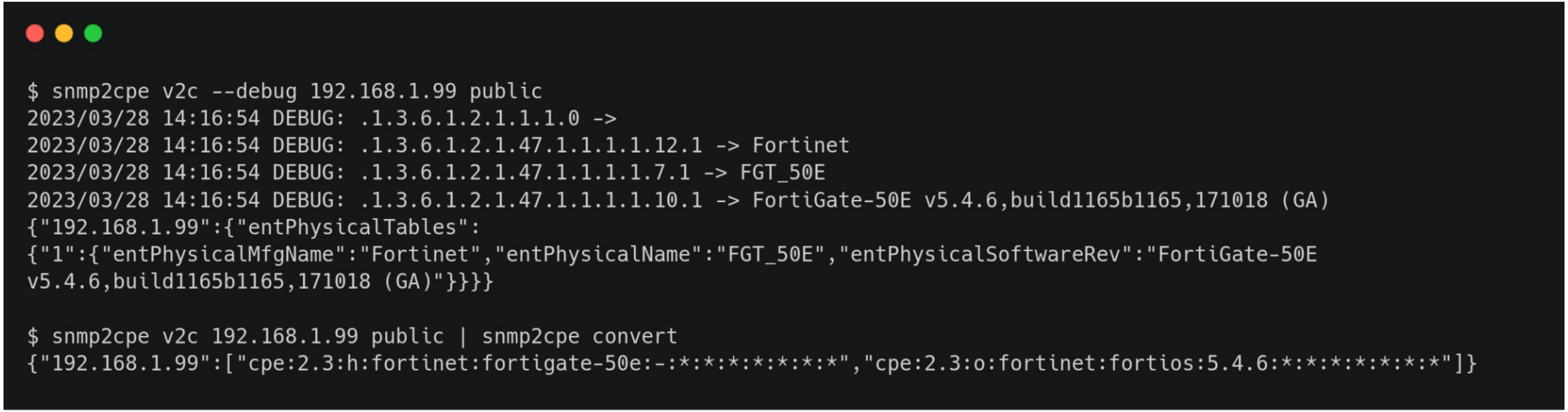
# より利用可能な脆弱性アドバイザリを提供するために

- 安定して定期的に取得可能である
  - API でアドバイザリ名、アドバイザリ本体を提供
  - Index of のようなリストで脆弱性アドバイザリを提供
  - 年単位などで脆弱性アドバイザリを一つにまとめて提供
  - Git Repository で提供
- 機械的に処理する前提のフォーマットを採用する
  - CVRF/CSAF 、 OVAL 、 MITRE CVE 、 OSV など脆弱性情報を記述するフォーマットは沢山ある
- アドバイザリ全体で記述が一意に定まっている
  - 古いものから新しいものの全てで、どこに何を書くか、どう表現するかが統一されている
- 公開したアドバイザリからセキュリティ製品を作れるか？という視点を持つ
  - 内容は十分ですか？適切に更新してますか？

# ネットワーク機器の特定 (SNMP)

# SNMP を用いたネットワーク機器の特定

sysDescr, entPhysicalMfgName, entPhysicalName, entPhysicalSoftwareRev から CPE へ



```
$ snmp2cpe v2c --debug 192.168.1.99 public
2023/03/28 14:16:54 DEBUG: .1.3.6.1.2.1.1.1.0 ->
2023/03/28 14:16:54 DEBUG: .1.3.6.1.2.1.47.1.1.1.1.12.1 -> Fortinet
2023/03/28 14:16:54 DEBUG: .1.3.6.1.2.1.47.1.1.1.1.7.1 -> FGT_50E
2023/03/28 14:16:54 DEBUG: .1.3.6.1.2.1.47.1.1.1.1.10.1 -> FortiGate-50E v5.4.6,build1165b1165,171018 (GA)
{"192.168.1.99":{"entPhysicalTables":
{"1":{"entPhysicalMfgName":"Fortinet","entPhysicalName":"FGT_50E","entPhysicalSoftwareRev":"FortiGate-50E
v5.4.6,build1165b1165,171018 (GA)"}}}}

$ snmp2cpe v2c 192.168.1.99 public | snmp2cpe convert
{"192.168.1.99":["cpe:2.3:h:fortinet:fortigate-50e:-:*:*:*:*:*:*:*","cpe:2.3:o:fortinet:fortios:5.4.6:*:*:*:*:*:*:*"]}
```

https://github.com/future-architect/vuls/tree/master/contrib/snmp2cpe

# ネットワーク機器の特定での課題

同じベンダ製品でも標準 MIB の記述が統一されていないため、どの情報を使えば安定するか分からない
（SNMP のサンプルが圧倒的に足りていない……

- ○ Juniper Networks MX240
  - ■ sysDescr.0: Juniper Networks, Inc. mx240 internet router, kernel JUNOS 20.4R3-S4.8, Build date: 2022-08-16 20:42:11 UTC Copyright (c) 1996-2022 Juniper Networks, Inc.
  - ■ entPhysicalMfgName.1: Juniper Networks
  - ■ entPhysicalName.1: CHAS-BP3-MX240-S
  - ■ entPhysicalSoftwareRev.1: 20.4R3-S4.8
- ○ Juniper Networks SRX4600
  - ■ sysDescr.0: Juniper Networks, Inc. srx4600 internet router, kernel JUNOS 20.4R3-S4.8, Build date: 2022-08-16 20:42:11 UTC Copyright (c) 1996-2022 Juniper Networks, Inc.
  - ■ entPhysicalMfgName.1:
  - ■ entPhysicalName.1:
  - ■ entPhysicalSoftwareRev.1:
- ○ Juniper Networks EX4300-32F
  - ■ sysDescr.0: Juniper Networks, Inc. ex4300-32f Ethernet Switch, kernel JUNOS 20.4R3-S4.8, Build date: 2022-08-16 21:10:45 UTC Copyright (c) 1996-2022 Juniper Networks, Inc.
  - ■ entPhysicalMfgName.1: Juniper Networks
  - ■ entPhysicalName.1:
  - ■ entPhysicalSoftwareRev.1: 20.4R3-S4.8

https://github.com/future-architect/vuls/blob/master/contrib/snmp2cpe/pkg/cpe/cpe_test.go

# まとめ

# 体感・課題

脆弱性アドバイザリの収集

- 機械的に収集することが難しく、活用まで届いていない
  - 脆弱性アドバイザリは利用されることに価値がある
  - 特に機械的に収集して、脆弱性 DB を作成することが主流
  - 脆弱性スキャナの NW 機器への対応状況から、アドバイザリが活用されていない様に感じる

ネットワーク機器の特定 (SNMP)

- 標準 MIB だけを使った現手法では、精度を保証することが難しい
- 汎用的に特定するにはサンプル数が圧倒的に足りていない

# 議論

NW 機器の脆弱性管理どうしてますか？

- 脆弱性検知・トリアージの頻度や方法は？機器情報の管理は？

脆弱性アドバイザリ

- 自社の脆弱性アドバイザリの現状を知っていましたか？
  （もし、改善したい・意見を聞きたいなどは @MaineK00n へ！
- 提供されている脆弱性アドバイザリをどのように利用している？
  （加工して利用しているのであれば、それを公開して、コミュニティ全体でメンテナンスするなどに興味はある？

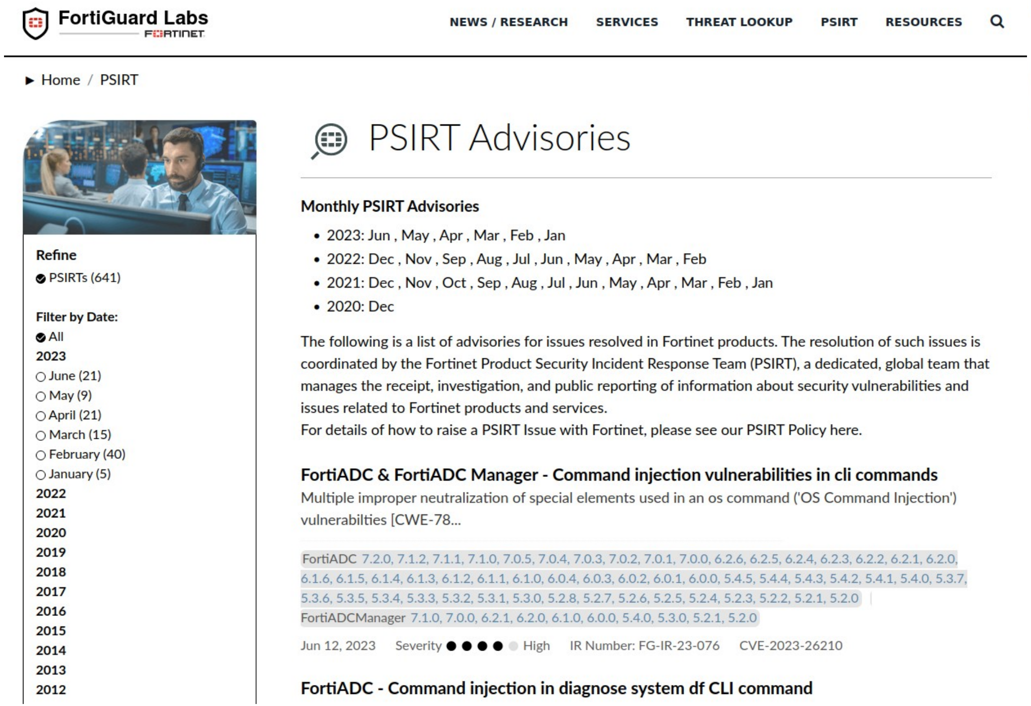
ネットワーク機器の特定

- 汎用的に複数台を特定するとして、SNMP より良い手法がある？
- SNMP なら、拡張 MIB まで見なければならない？
- 精度を保証するためにテストケースを集めるには？

# Appendix A:
# 脆弱性アドバイザリの提供状況と特徴
# @ 2023/06/15

# fortinet

# 総アドバイザリ数 : 636 / ページネーション / Web, CVRF



▸ Home / PSIRT

## PSIRT Advisories

Refine

● PSIRTs (641)

Filter by Date:

● All

2023

○ June (21)

○ May (9)

○ April (21)

○ March (15)

○ February (40)

○ January (5)

2022

2021

2020

2019

2018

2017

2016

2015

2014

2013

2012

**Monthly PSIRT Advisories**

- 2023: Jun , May , Apr , Mar , Feb , Jan
- 2022: Dec , Nov , Sep , Aug , Jul , Jun , May , Apr , Mar , Feb
- 2021: Dec , Nov , Oct , Sep , Aug , Jul , Jun , May , Apr , Mar , Feb , Jan
- 2020: Dec

The following is a list of advisories for issues resolved in Fortinet products. The resolution of such issues is coordinated by the Fortinet Product Security Incident Response Team (PSIRT), a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Fortinet products and services.
For details of how to raise a PSIRT Issue with Fortinet, please see our PSIRT Policy here.

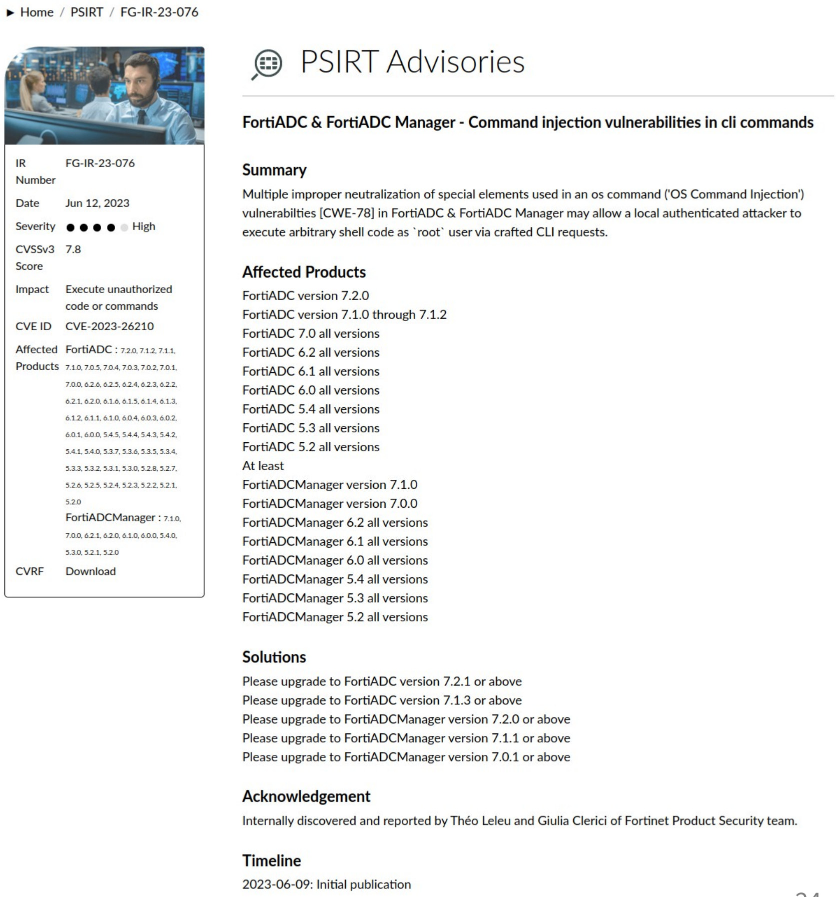
**FortiADC & FortiADC Manager - Command injection vulnerabilities in cli commands**

Multiple improper neutralization of special elements used in an os command ('OS Command Injection') vulnerabilties [CWE-78...

FortiADC 7.2.0, 7.1.2, 7.1.1, 7.1.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.1.6, 6.1.5, 6.1.4, 6.1.3, 6.1.2, 6.1.1, 6.1.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.1, 5.4.0, 5.3.7, 5.3.6, 5.3.5, 5.3.4, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.4, 5.2.3, 5.2.2, 5.2.1, 5.2.0 | FortiADCManager 7.1.0, 7.0.0, 6.2.1, 6.2.0, 6.1.0, 6.0.0, 5.4.0, 5.3.0, 5.2.1, 5.2.0

Jun 12, 2023 Severity ●●●●○ High IR Number: FG-IR-23-076 CVE-2023-26210

**FortiADC - Command injection in diagnose system df CLI command**



▸ Home / PSIRT / FG-IR-23-076

| | |
|---|---|
| IR Number | FG-IR-23-076 |
| Date | Jun 12, 2023 |
| Severity | ●●●●○ High |
| CVSSv3 Score | 7.8 |
| Impact | Execute unauthorized code or commands |
| CVE ID | CVE-2023-26210 |
| Affected Products | FortiADC : 7.2.0, 7.1.2, 7.1.1, 7.1.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.1.6, 6.1.5, 6.1.4, 6.1.3, 6.1.2, 6.1.1, 6.1.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.1, 5.4.0, 5.3.7, 5.3.6, 5.3.5, 5.3.4, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.4, 5.2.3, 5.2.2, 5.2.1, 5.2.0<br>FortiADCManager : 7.1.0, 7.0.0, 6.2.1, 6.2.0, 6.1.0, 6.0.0, 5.4.0, 5.3.0, 5.2.1, 5.2.0 |
| CVRF | Download |

## PSIRT Advisories

**FortiADC & FortiADC Manager - Command injection vulnerabilities in cli commands**

**Summary**

Multiple improper neutralization of special elements used in an os command ('OS Command Injection') vulnerabilties [CWE-78] in FortiADC & FortiADC Manager may allow a local authenticated attacker to execute arbitrary shell code as `root` user via crafted CLI requests.

**Affected Products**

FortiADC version 7.2.0
FortiADC version 7.1.0 through 7.1.2
FortiADC 7.0 all versions
FortiADC 6.2 all versions
FortiADC 6.1 all versions
FortiADC 6.0 all versions
FortiADC 5.4 all versions
FortiADC 5.3 all versions
FortiADC 5.2 all versions
At least
FortiADCManager version 7.1.0
FortiADCManager version 7.0.0
FortiADCManager 6.2 all versions
FortiADCManager 6.1 all versions
FortiADCManager 6.0 all versions
FortiADCManager 5.4 all versions
FortiADCManager 5.3 all versions
FortiADCManager 5.2 all versions

**Solutions**

Please upgrade to FortiADC version 7.2.1 or above
Please upgrade to FortiADC version 7.1.3 or above
Please upgrade to FortiADCManager version 7.2.0 or above
Please upgrade to FortiADCManager version 7.1.1 or above
Please upgrade to FortiADCManager version 7.0.1 or above

**Acknowledgement**

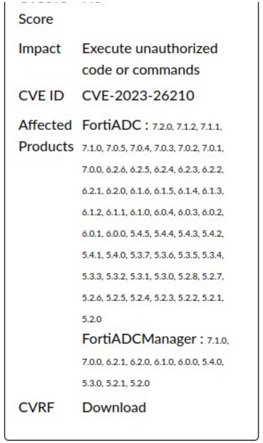
Internally discovered and reported by Théo Leleu and Giulia Clerici of Fortinet Product Security team.

**Timeline**

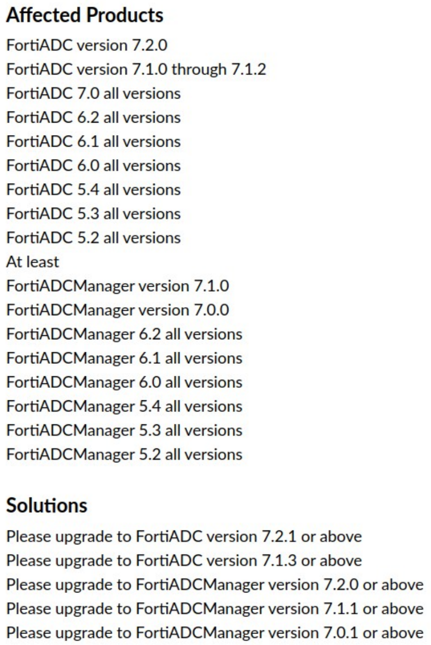
2023-06-09: Initial publication

https://www.fortiguard.com/psirt

# CVRF ProductTree ではなく、 Notes に Affected と Fixed Version を記述



| | |
|---|---|
| Score | |
| Impact | Execute unauthorized code or commands |
| CVE ID | CVE-2023-26210 |
| Affected Products | FortiADC : 7.2.0, 7.1.2, 7.1.1, 7.1.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.1.6, 6.1.5, 6.1.4, 6.1.3, 6.1.2, 6.1.1, 6.1.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.1, 5.4.0, 5.3.7, 5.3.6, 5.3.5, 5.3.4, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.4, 5.2.3, 5.2.2, 5.2.1, 5.2.0<br>FortiADCManager : 7.1.0, 7.0.0, 6.2.1, 6.2.0, 6.1.0, 6.0.0, 5.4.0, 5.3.0, 5.2.1, 5.2.0 |
| CVRF | Download |

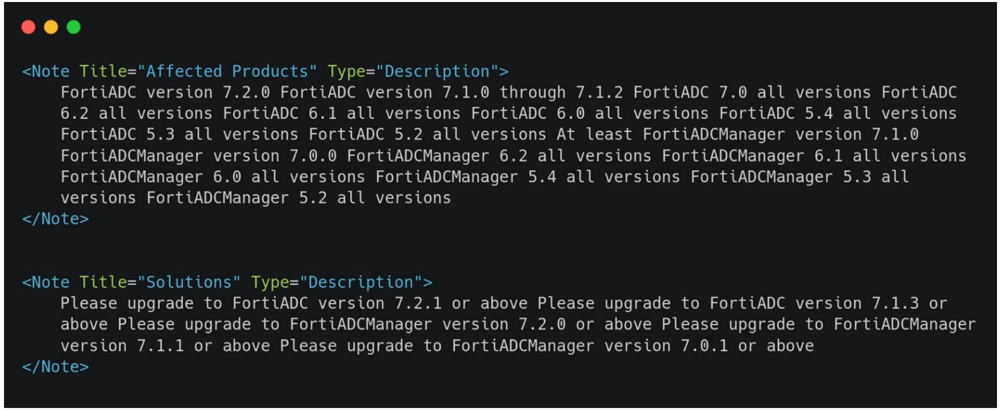


## Affected Products

FortiADC version 7.2.0
FortiADC version 7.1.0 through 7.1.2
FortiADC 7.0 all versions
FortiADC 6.2 all versions
FortiADC 6.1 all versions
FortiADC 6.0 all versions
FortiADC 5.4 all versions
FortiADC 5.3 all versions
FortiADC 5.2 all versions
At least
FortiADCManager version 7.1.0
FortiADCManager version 7.0.0
FortiADCManager 6.2 all versions
FortiADCManager 6.1 all versions
FortiADCManager 6.0 all versions
FortiADCManager 5.4 all versions
FortiADCManager 5.3 all versions
FortiADCManager 5.2 all versions

## Solutions

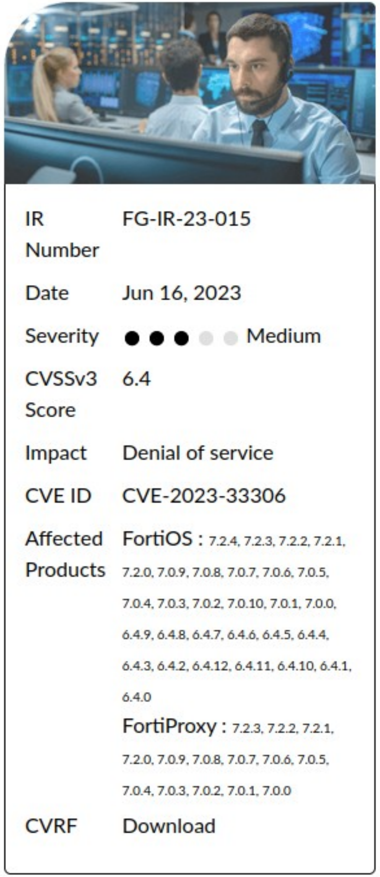
Please upgrade to FortiADC version 7.2.1 or above
Please upgrade to FortiADC version 7.1.3 or above
Please upgrade to FortiADCManager version 7.2.0 or above
Please upgrade to FortiADCManager version 7.1.1 or above
Please upgrade to FortiADCManager version 7.0.1 or above



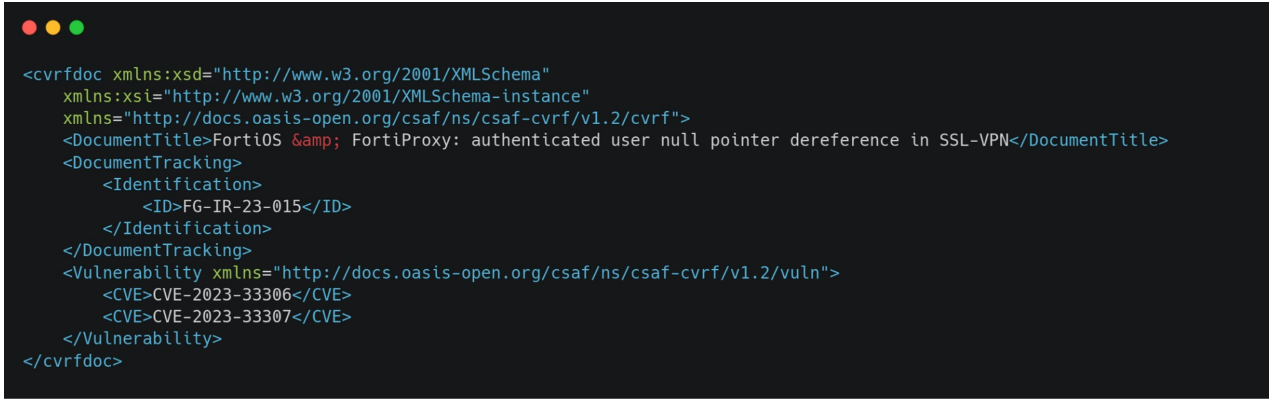
```
<Note Title="Affected Products" Type="Description">
    FortiADC version 7.2.0 FortiADC version 7.1.0 through 7.1.2 FortiADC 7.0 all versions FortiADC
    6.2 all versions FortiADC 6.1 all versions FortiADC 6.0 all versions FortiADC 5.4 all versions
    FortiADC 5.3 all versions FortiADC 5.2 all versions At least FortiADCManager version 7.1.0
    FortiADCManager version 7.0.0 FortiADCManager 6.2 all versions FortiADCManager 6.1 all versions
    FortiADCManager 6.0 all versions FortiADCManager 5.4 all versions FortiADCManager 5.3 all
    versions FortiADCManager 5.2 all versions
</Note>


<Note Title="Solutions" Type="Description">
    Please upgrade to FortiADC version 7.2.1 or above Please upgrade to FortiADC version 7.1.3 or
    above Please upgrade to FortiADCManager version 7.2.0 or above Please upgrade to FortiADCManager
    version 7.1.1 or above Please upgrade to FortiADCManager version 7.0.1 or above
</Note>
```

[1] https://www.fortiguard.com/psirt/FG-IR-23-076 [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-23-076

# 複数 CVE が紐付いている場合、 CVRF にしか書いてない



| | |
|---|---|
| IR Number | FG-IR-23-015 |
| Date | Jun 16, 2023 |
| Severity | ●●●○○ Medium |
| CVSSv3 Score | 6.4 |
| Impact | Denial of service |
| CVE ID | CVE-2023-33306 |
| Affected Products | FortiOS : 7.2.4, 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.10, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.12, 6.4.11, 6.4.10, 6.4.1, 6.4.0<br>FortiProxy : 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0 |
| CVRF | Download |

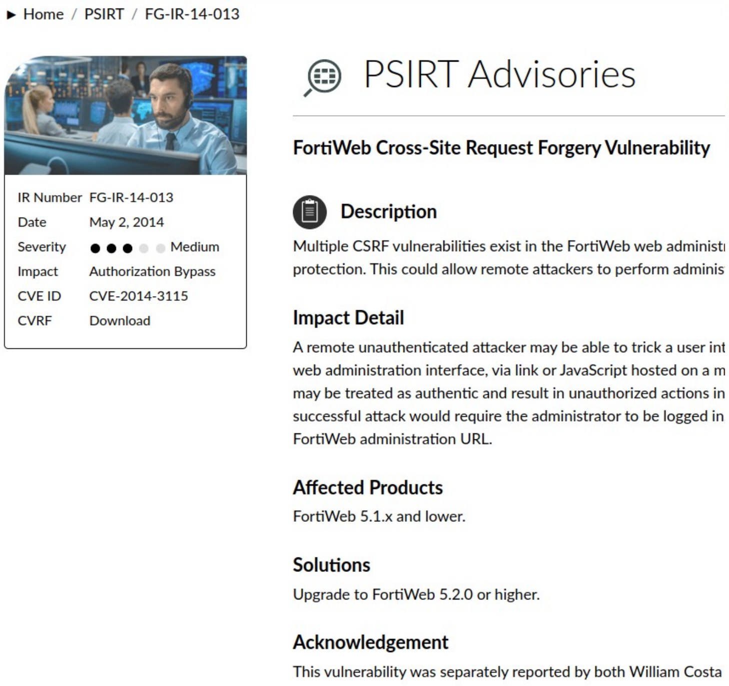


```
<cvrfdoc xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/cvrf">
    <DocumentTitle>FortiOS &amp; FortiProxy: authenticated user null pointer dereference in SSL-VPN</DocumentTitle>
    <DocumentTracking>
        <Identification>
            <ID>FG-IR-23-015</ID>
        </Identification>
    </DocumentTracking>
    <Vulnerability xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/vuln">
        <CVE>CVE-2023-33306</CVE>
        <CVE>CVE-2023-33307</CVE>
    </Vulnerability>
</cvrfdoc>
```

[1] https://www.fortiguard.com/psirt/FG-IR-23-015 [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-23-015

# サイドバーの Affected Products がない場合、 all versions を調べることが大変

## FortiWeb 5.1 系の最終リリースって？他アドバイザリやドキュメント的に 5.1.4?



► Home / PSIRT / FG-IR-14-013

| | |
|---|---|
| IR Number | FG-IR-14-013 |
| Date | May 2, 2014 |
| Severity | ● ● ● ○ ○ Medium |
| Impact | Authorization Bypass |
| CVE ID | CVE-2014-3115 |
| CVRF | Download |

PSIRT Advisories

**FortiWeb Cross-Site Request Forgery Vulnerability**

**Description**

Multiple CSRF vulnerabilities exist in the FortiWeb web administi
protection. This could allow remote attackers to perform adminis

**Impact Detail**

A remote unauthenticated attacker may be able to trick a user int
web administration interface, via link or JavaScript hosted on a m
may be treated as authentic and result in unauthorized actions in
successful attack would require the administrator to be logged in
FortiWeb administration URL.

**Affected Products**

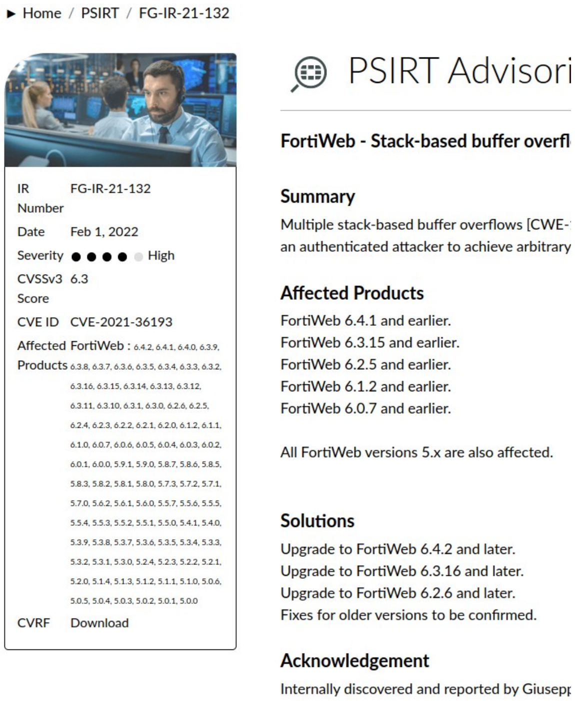
FortiWeb 5.1.x and lower.

**Solutions**

Upgrade to FortiWeb 5.2.0 or higher.

**Acknowledgement**

This vulnerability was separately reported by both William Costa



► Home / PSIRT / FG-IR-21-132

| | |
|---|---|
| IR Number | FG-IR-21-132 |
| Date | Feb 1, 2022 |
| Severity | ● ● ● ● ○ High |
| CVSSv3 Score | 6.3 |
| CVE ID | CVE-2021-36193 |
| Affected Products | FortiWeb : 6.4.2, 6.4.1, 6.4.0, 6.3.9, 6.3.8, 6.3.7, 6.3.6, 6.3.5, 6.3.4, 6.3.3, 6.3.2, 6.3.16, 6.3.15, 6.3.14, 6.3.13, 6.3.12, 6.3.11, 6.3.10, 6.3.1, 6.3.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.1.2, 6.1.1, 6.1.0, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.9.1, 5.9.0, 5.8.7, 5.8.6, 5.8.5, 5.8.3, 5.8.2, 5.8.1, 5.8.0, 5.7.3, 5.7.2, 5.7.1, 5.7.0, 5.6.2, 5.6.1, 5.6.0, 5.5.7, 5.5.6, 5.5.5, 5.5.4, 5.5.3, 5.5.2, 5.5.1, 5.5.0, 5.4.1, 5.4.0, 5.3.9, 5.3.8, 5.3.7, 5.3.6, 5.3.5, 5.3.4, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.4, 5.2.3, 5.2.2, 5.2.1, 5.2.0, 5.1.4, 5.1.3, 5.1.2, 5.1.1, 5.1.0, 5.0.6, 5.0.5, 5.0.4, 5.0.3, 5.0.2, 5.0.1, 5.0.0 |
| CVRF | Download |

PSIRT Advisori

**FortiWeb - Stack-based buffer overfl**

**Summary**

Multiple stack-based buffer overflows [CWE-
an authenticated attacker to achieve arbitrary

**Affected Products**

FortiWeb 6.4.1 and earlier.
FortiWeb 6.3.15 and earlier.
FortiWeb 6.2.5 and earlier.
FortiWeb 6.1.2 and earlier.
FortiWeb 6.0.7 and earlier.

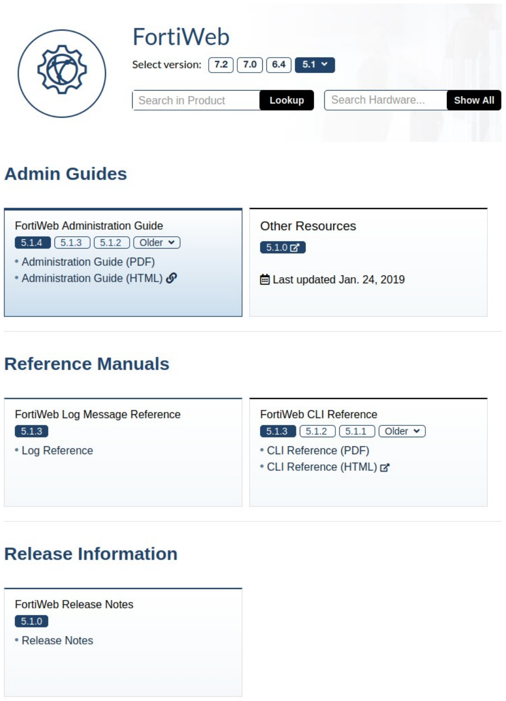
All FortiWeb versions 5.x are also affected.

**Solutions**

Upgrade to FortiWeb 6.4.2 and later.
Upgrade to FortiWeb 6.3.16 and later.
Upgrade to FortiWeb 6.2.6 and later.
Fixes for older versions to be confirmed.

**Acknowledgement**

Internally discovered and reported by Giusepp



FortiWeb

Select version: 7.2 7.0 6.4 5.1

**Admin Guides**

FortiWeb Administration Guide
5.1.4 5.1.3 5.1.2 Older
- Administration Guide (PDF)
- Administration Guide (HTML)

Other Resources
5.1.0
Last updated Jan. 24, 2019

**Reference Manuals**

FortiWeb Log Message Reference
5.1.3
- Log Reference

FortiWeb CLI Reference
5.1.3 5.1.2 5.1.1 Older
- CLI Reference (PDF)
- CLI Reference (HTML)

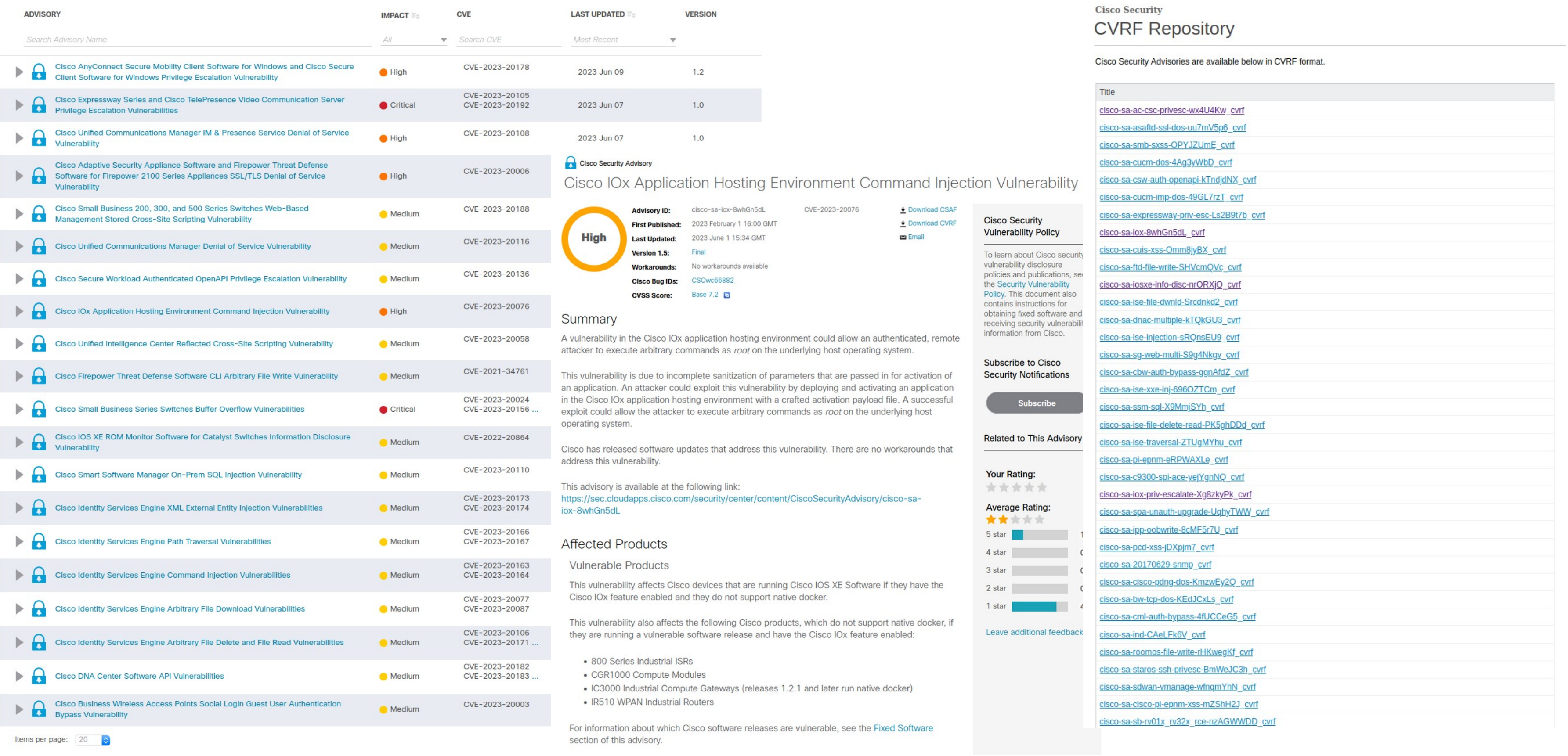
**Release Information**

FortiWeb Release Notes
5.1.0
- Release Notes

[1] https://www.fortiguard.com/psirt/FG-IR-14-013 [2] https://www.fortiguard.com/psirt/FG-IR-21-132 [3] https://docs.fortinet.com/index.php/product/fortiweb/5.1

# Cisco Systems

# 総アドバイザリ数 : 4691 / ページネーション [1], リスト [2] / Web, CVRF, CSAF



| ADVISORY | IMPACT | CVE | LAST UPDATED | VERSION |
|---|---|---|---|---|
| Search Advisory Name | All | Search CVE | Most Recent | |
| Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability | ● High | CVE-2023-20178 | 2023 Jun 09 | 1.2 |
| Cisco Expressway Series and Cisco TelePresence Video Communication Server Privilege Escalation Vulnerabilities | ● Critical | CVE-2023-20105<br>CVE-2023-20192 | 2023 Jun 07 | 1.0 |
| Cisco Unified Communications Manager IM & Presence Service Denial of Service Vulnerability | ● High | CVE-2023-20108 | 2023 Jun 07 | 1.0 |
| Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS Denial of Service Vulnerability | ● High | CVE-2023-20006 | | |
| Cisco Small Business 200, 300, and 500 Series Switches Web-Based Management Stored Cross-Site Scripting Vulnerability | ● Medium | CVE-2023-20188 | | |
| Cisco Unified Communications Manager Denial of Service Vulnerability | ● Medium | CVE-2023-20116 | | |
| Cisco Secure Workload Authenticated OpenAPI Privilege Escalation Vulnerability | ● Medium | CVE-2023-20136 | | |
| Cisco IOx Application Hosting Environment Command Injection Vulnerability | ● High | CVE-2023-20076 | | |
| Cisco Unified Intelligence Center Reflected Cross-Site Scripting Vulnerability | ● Medium | CVE-2023-20058 | | |
| Cisco Firepower Threat Defense Software CLI Arbitrary File Write Vulnerability | ● Medium | CVE-2021-34761 | | |
| Cisco Small Business Series Switches Buffer Overflow Vulnerabilities | ● Critical | CVE-2023-20024<br>CVE-2023-20156 ... | | |
| Cisco IOS XE ROM Monitor Software for Catalyst Switches Information Disclosure Vulnerability | ● Medium | CVE-2022-20864 | | |
| Cisco Smart Software Manager On-Prem SQL Injection Vulnerability | ● Medium | CVE-2023-20110 | | |
| Cisco Identity Services Engine XML External Entity Injection Vulnerabilities | ● Medium | CVE-2023-20173<br>CVE-2023-20174 | | |
| Cisco Identity Services Engine Path Traversal Vulnerabilities | ● Medium | CVE-2023-20166<br>CVE-2023-20167 | | |
| Cisco Identity Services Engine Command Injection Vulnerabilities | ● Medium | CVE-2023-20163<br>CVE-2023-20164 | | |
| Cisco Identity Services Engine Arbitrary File Download Vulnerabilities | ● Medium | CVE-2023-20077<br>CVE-2023-20087 | | |
| Cisco Identity Services Engine Arbitrary File Delete and File Read Vulnerabilities | ● Medium | CVE-2023-20106<br>CVE-2023-20171 ... | | |
| Cisco DNA Center Software API Vulnerabilities | ● Medium | CVE-2023-20182<br>CVE-2023-20183 ... | | |
| Cisco Business Wireless Access Points Social Login Guest User Authentication Bypass Vulnerability | ● Medium | CVE-2023-20003 | | |

Items per page: 20

Cisco Security Advisory

## Cisco IOx Application Hosting Environment Command Injection Vulnerability

High

| | | |
|---|---|---|
| Advisory ID: | cisco-sa-iox-8whGn5dL | CVE-2023-20076 |
| First Published: | 2023 February 1 16:00 GMT | |
| Last Updated: | 2023 June 1 15:34 GMT | |
| Version 1.5: | Final | |
| Workarounds: | No workarounds available | |
| Cisco Bug IDs: | CSCwc66882 | |
| CVSS Score: | Base 7.2 | |

Download CSAF
Download CVRF
Email

### Summary

A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as *root* on the underlying host operating system.

This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as *root* on the underlying host operating system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL

### Affected Products

Vulnerable Products

This vulnerability affects Cisco devices that are running Cisco IOS XE Software if they have the Cisco IOx feature enabled and they do not support native docker.

This vulnerability also affects the following Cisco products, which do not support native docker, if they are running a vulnerable software release and have the Cisco IOx feature enabled:

- 800 Series Industrial ISRs
- CGR1000 Compute Modules
- IC3000 Industrial Compute Gateways (releases 1.2.1 and later run native docker)
- IR510 WPAN Industrial Routers

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Cisco Security Vulnerability Policy

To learn about Cisco securit vulnerability disclosure policies and publications, se the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerabilit information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Related to This Advisory

Your Rating:

Average Rating:

| | | |
|---|---|---|
| 5 star | | 1 |
| 4 star | | 0 |
| 3 star | | 0 |
| 2 star | | 0 |
| 1 star | | 4 |

Leave additional feedback

Cisco Security

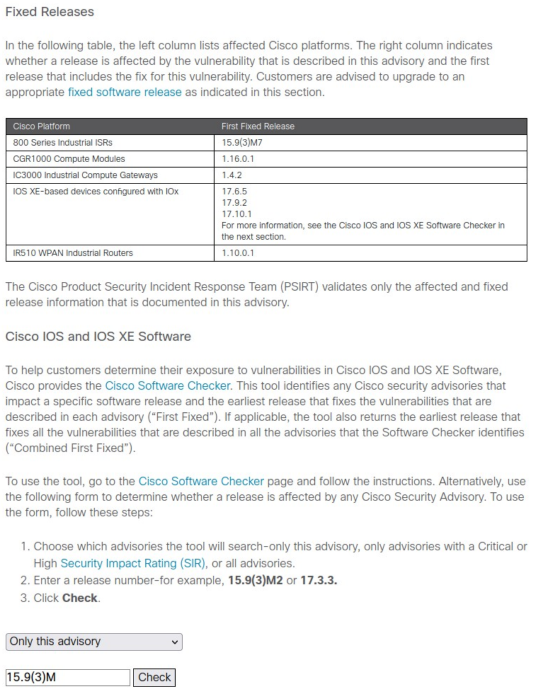
## CVRF Repository

Cisco Security Advisories are available below in CVRF format.

| Title |
|---|
| cisco-sa-ac-csc-privesc-wx4U4Kw_cvrf |
| cisco-sa-asaftd-ssl-dos-uu7mV5p6_cvrf |
| cisco-sa-smb-sxss-OPYJZUmE_cvrf |
| cisco-sa-cucm-dos-4Ag3yWbD_cvrf |
| cisco-sa-csw-auth-openapi-kTndjdNX_cvrf |
| cisco-sa-cucm-imp-dos-49GL7rzT_cvrf |
| cisco-sa-expressway-priv-esc-Ls2B9t7b_cvrf |
| cisco-sa-iox-8whGn5dL_cvrf |
| cisco-sa-cuis-xss-Omm8jyBX_cvrf |
| cisco-sa-ftd-file-write-SHVcmQVc_cvrf |
| cisco-sa-iosxe-info-disc-nrORXjO_cvrf |
| cisco-sa-ise-file-dwnld-Srcdnkd2_cvrf |
| cisco-sa-dnac-multiple-kTQkGU3_cvrf |
| cisco-sa-ise-injection-sRQnsEU9_cvrf |
| cisco-sa-sg-web-multi-S9g4Nkgv_cvrf |
| cisco-sa-cbw-auth-bypass-ggnAfdZ_cvrf |
| cisco-sa-ise-xxe-inj-696OZTCm_cvrf |
| cisco-sa-ssm-sql-X9MmjSYh_cvrf |
| cisco-sa-ise-file-delete-read-PK5ghDDd_cvrf |
| cisco-sa-ise-traversal-ZTUgMYhu_cvrf |
| cisco-sa-pi-epnm-eRPWAXLe_cvrf |
| cisco-sa-c9300-spi-ace-yejYgnNQ_cvrf |
| cisco-sa-iox-priv-escalate-Xg8zkyPk_cvrf |
| cisco-sa-spa-unauth-upgrade-UqhyTWW_cvrf |
| cisco-sa-ipp-oobwrite-8cMF5r7U_cvrf |
| cisco-sa-pcd-xss-jDXpjm7_cvrf |
| cisco-sa-20170629-snmp_cvrf |
| cisco-sa-cisco-pdng-dos-KmzwEy2Q_cvrf |
| cisco-sa-bw-tcp-dos-KEdJCxLs_cvrf |
| cisco-sa-cml-auth-bypass-4fUCCeG5_cvrf |
| cisco-sa-ind-CAeLFk6V_cvrf |
| cisco-sa-roomos-file-write-rHKwegKf_cvrf |
| cisco-sa-staros-ssh-privesc-BmWeJC3h_cvrf |
| cisco-sa-sdwan-vmanage-wfnqmYhN_cvrf |
| cisco-sa-cisco-pi-epnm-xss-mZShH2J_cvrf |
| cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD_cvrf |

[1] https://sec.cloudapps.cisco.com/security/center/publicationListing.x [2] https://sec.cloudapps.cisco.com/security/center/cvrfListing.x

# Cisco Software Checker でなければ fixed version が分からない（IOS and IOS XE Software



### Fixed Releases

In the following table, the left column lists affected Cisco platforms. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

| Cisco Platform | First Fixed Release |
|---|---|
| 800 Series Industrial ISRs | 15.9(3)M7 |
| CGR1000 Compute Modules | 1.16.0.1 |
| IC3000 Industrial Compute Gateways | 1.4.2 |
| IOS XE-based devices configured with IOx | 17.6.5<br>17.9.2<br>17.10.1<br>For more information, see the Cisco IOS and IOS XE Software Checker in the next section. |
| IR510 WPAN Industrial Routers | 1.10.0.1 |

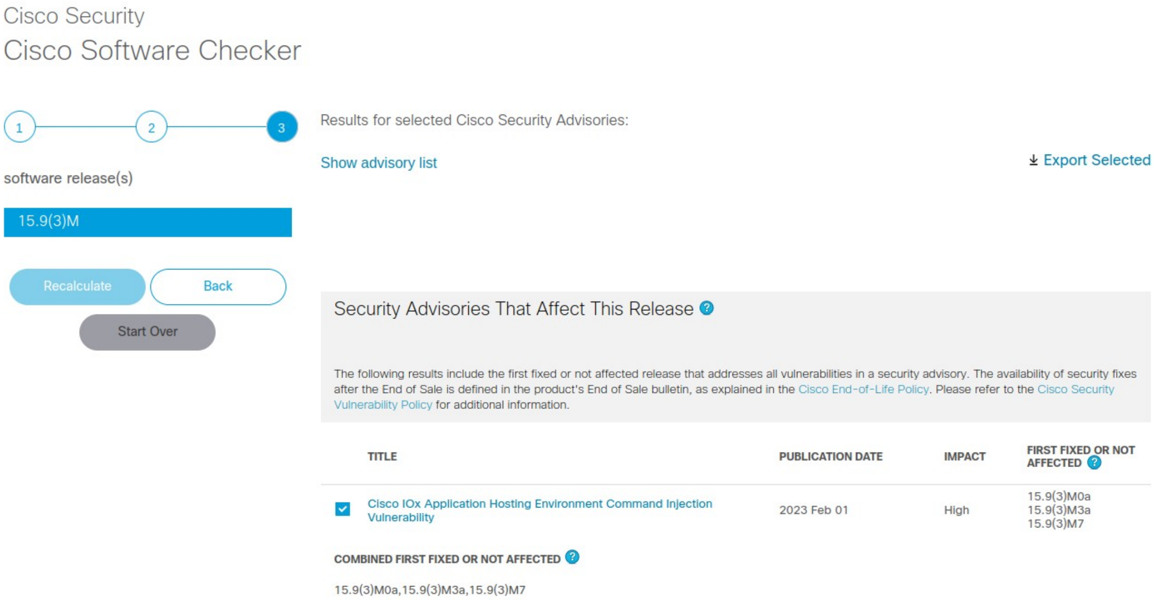
The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

### Cisco IOS and IOS XE Software

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described in each advisory ("First Fixed"). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities that are described in all the advisories that the Software Checker identifies ("Combined First Fixed").

To use the tool, go to the Cisco Software Checker page and follow the instructions. Alternatively, use the following form to determine whether a release is affected by any Cisco Security Advisory. To use the form, follow these steps:

1. Choose which advisories the tool will search-only this advisory, only advisories with a Critical or High Security Impact Rating (SIR), or all advisories.
2. Enter a release number-for example, **15.9(3)M2** or **17.3.3.**
3. Click **Check**.



Cisco Security

## Cisco Software Checker

software release(s)

15.9(3)M

Results for selected Cisco Security Advisories:

### Security Advisories That Affect This Release

The following results include the first fixed or not affected release that addresses all vulnerabilities in a security advisory. The availability of security fixes after the End of Sale is defined in the product's End of Sale bulletin, as explained in the Cisco End-of-Life Policy. Please refer to the Cisco Security Vulnerability Policy for additional information.

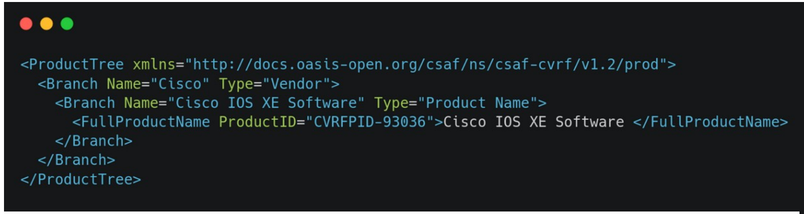
| | TITLE | PUBLICATION DATE | IMPACT | FIRST FIXED OR NOT AFFECTED |
|---|---|---|---|---|
| ☑ | Cisco IOx Application Hosting Environment Command Injection Vulnerability | 2023 Feb 01 | High | 15.9(3)M0a<br>15.9(3)M3a<br>15.9(3)M7 |

COMBINED FIRST FIXED OR NOT AFFECTED

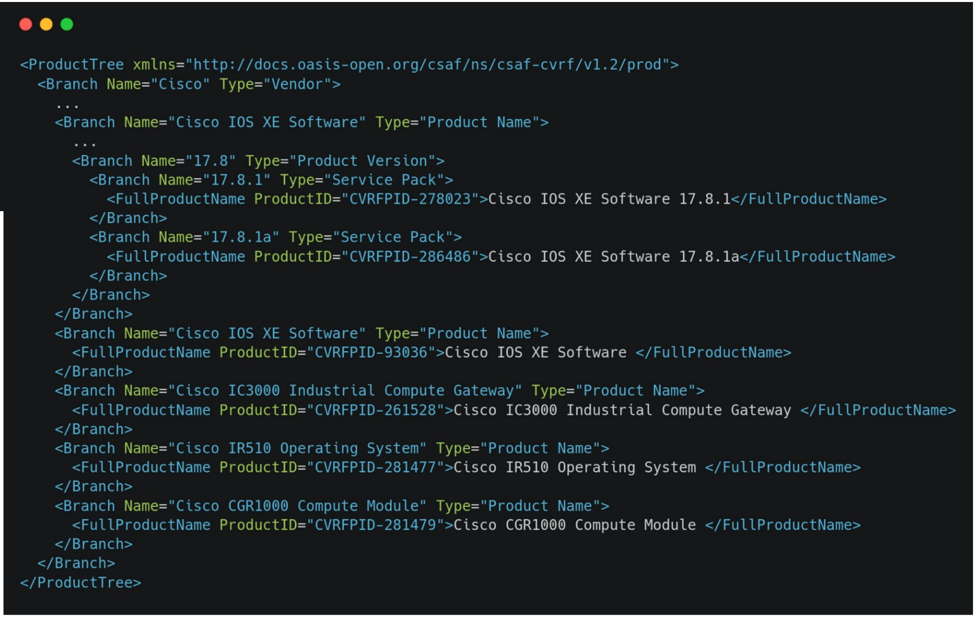
15.9(3)M0a,15.9(3)M3a,15.9(3)M7

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL

# Product Tree の情報量にばらつき



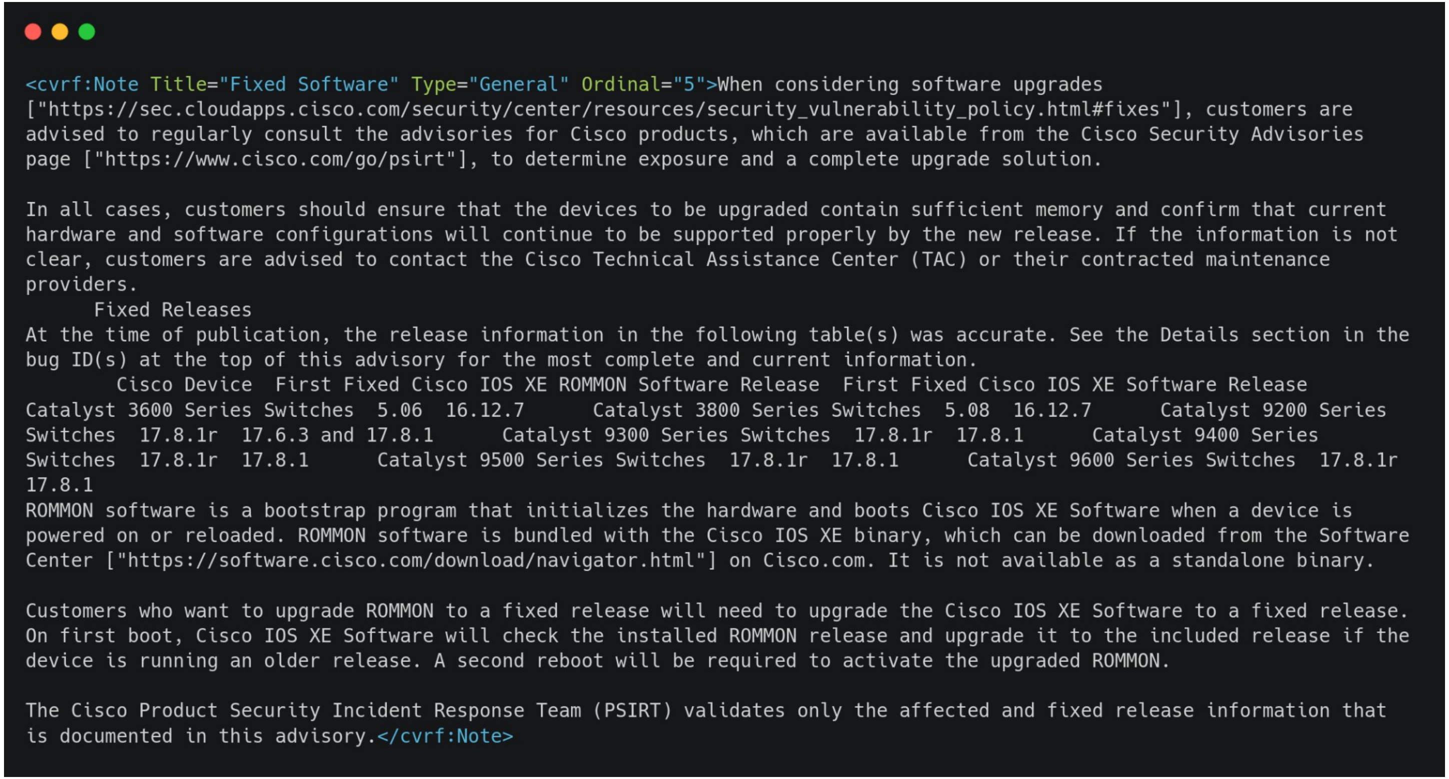
```
<ProductTree xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/prod">
  <Branch Name="Cisco" Type="Vendor">
    <Branch Name="Cisco IOS XE Software" Type="Product Name">
      <FullProductName ProductID="CVRFPID-93036">Cisco IOS XE Software </FullProductName>
    </Branch>
  </Branch>
</ProductTree>
```



```
<ProductTree xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/prod">
  <Branch Name="Cisco" Type="Vendor">
    ...
    <Branch Name="Cisco IOS XE Software" Type="Product Name">
      ...
      <Branch Name="17.8" Type="Product Version">
        <Branch Name="17.8.1" Type="Service Pack">
          <FullProductName ProductID="CVRFPID-278023">Cisco IOS XE Software 17.8.1</FullProductName>
        </Branch>
        <Branch Name="17.8.1a" Type="Service Pack">
          <FullProductName ProductID="CVRFPID-286486">Cisco IOS XE Software 17.8.1a</FullProductName>
        </Branch>
      </Branch>
    </Branch>
    <Branch Name="Cisco IOS XE Software" Type="Product Name">
      <FullProductName ProductID="CVRFPID-93036">Cisco IOS XE Software </FullProductName>
    </Branch>
    <Branch Name="Cisco IC3000 Industrial Compute Gateway" Type="Product Name">
      <FullProductName ProductID="CVRFPID-261528">Cisco IC3000 Industrial Compute Gateway </FullProductName>
    </Branch>
    <Branch Name="Cisco IR510 Operating System" Type="Product Name">
      <FullProductName ProductID="CVRFPID-281477">Cisco IR510 Operating System </FullProductName>
    </Branch>
    <Branch Name="Cisco CGR1000 Compute Module" Type="Product Name">
      <FullProductName ProductID="CVRFPID-281479">Cisco CGR1000 Compute Module </FullProductName>
    </Branch>
  </Branch>
</ProductTree>
```

[1] https://sec.cloudapps.cisco.com/security/center/contentxml/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO/cvrf/cisco-sa-iosxe-info-disc-nrORXjO_cvrf.xml
[2] https://sec.cloudapps.cisco.com/security/center/contentxml/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL/cvrf/cisco-sa-iox-8whGn5dL_cvrf.xml

# first fixed release が Note に書いてある

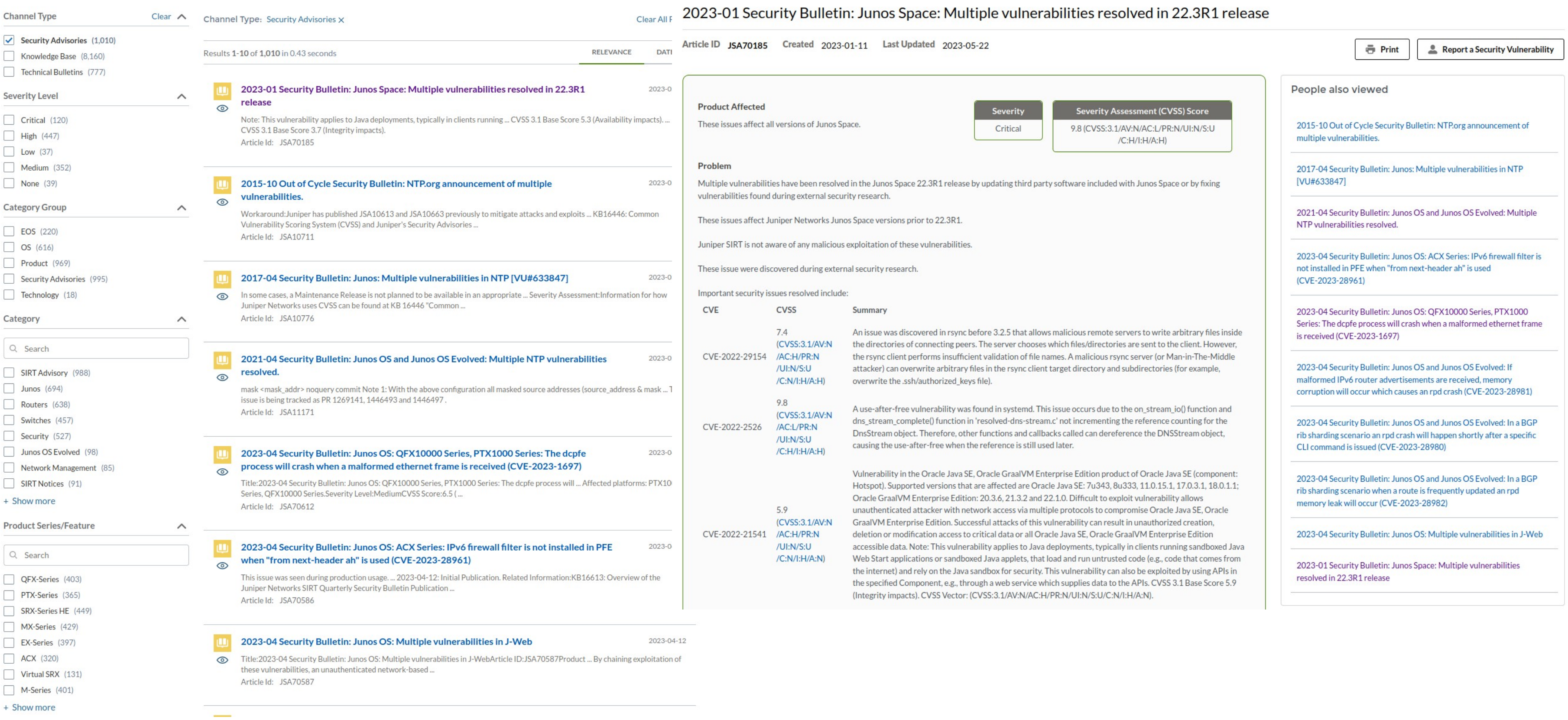


```
<cvrf:Note Title="Fixed Software" Type="General" Ordinal="5">When considering software upgrades
["https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes"], customers are
advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories
page ["https://www.cisco.com/go/psirt"], to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current
hardware and software configurations will continue to be supported properly by the new release. If the information is not
clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance
providers.
      Fixed Releases
At the time of publication, the release information in the following table(s) was accurate. See the Details section in the
bug ID(s) at the top of this advisory for the most complete and current information.
        Cisco Device  First Fixed Cisco IOS XE ROMMON Software Release  First Fixed Cisco IOS XE Software Release
Catalyst 3600 Series Switches  5.06  16.12.7      Catalyst 3800 Series Switches  5.08  16.12.7      Catalyst 9200 Series
Switches  17.8.1r  17.6.3 and 17.8.1      Catalyst 9300 Series Switches  17.8.1r  17.8.1      Catalyst 9400 Series
Switches  17.8.1r  17.8.1      Catalyst 9500 Series Switches  17.8.1r  17.8.1      Catalyst 9600 Series Switches  17.8.1r
17.8.1
ROMMON software is a bootstrap program that initializes the hardware and boots Cisco IOS XE Software when a device is
powered on or reloaded. ROMMON software is bundled with the Cisco IOS XE binary, which can be downloaded from the Software
Center ["https://software.cisco.com/download/navigator.html"] on Cisco.com. It is not available as a standalone binary.

Customers who want to upgrade ROMMON to a fixed release will need to upgrade the Cisco IOS XE Software to a fixed release.
On first boot, Cisco IOS XE Software will check the installed ROMMON release and upgrade it to the included release if the
device is running an older release. A second reboot will be required to activate the upgraded ROMMON.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that
is documented in this advisory.</cvrf:Note>
```

https://sec.cloudapps.cisco.com/security/center/contentxml/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO/cvrf/cisco-sa-iosxe-info-disc-nrORXjO_cvrf.xml

# Juniper Networks

# 総アドバイザリ数 : 1010 / ページネーション / Web



Channel Type  Clear

- ☑ Security Advisories (1,010)
- □ Knowledge Base (8,160)
- □ Technical Bulletins (777)

Severity Level

- □ Critical (120)
- □ High (447)
- □ Low (37)
- □ Medium (352)
- □ None (39)

Category Group

- □ EOS (220)
- □ OS (616)
- □ Product (969)
- □ Security Advisories (995)
- □ Technology (18)

Category

Search

- □ SIRT Advisory (988)
- □ Junos (694)
- □ Routers (638)
- □ Switches (457)
- □ Security (527)
- □ Junos OS Evolved (98)
- □ Network Management (85)
- □ SIRT Notices (91)

+ Show more

Product Series/Feature

Search

- □ QFX-Series (403)
- □ PTX-Series (365)
- □ SRX-Series HE (449)
- □ MX-Series (429)
- □ EX-Series (397)
- □ ACX (320)
- □ Virtual SRX (131)
- □ M-Series (401)

+ Show more

Channel Type: Security Advisories ✕  Clear All F

Results **1-10** of **1,010** in 0.43 seconds  RELEVANCE  DATI

**2023-01 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 22.3R1 release**  2023-0
Note: This vulnerability applies to Java deployments, typically in clients running ... CVSS 3.1 Base Score 5.3 (Availability impacts). ... CVSS 3.1 Base Score 3.7 (Integrity impacts).
Article Id: JSA70185

**2015-10 Out of Cycle Security Bulletin: NTP.org announcement of multiple vulnerabilities.**  2023-0
Workaround:Juniper has published JSA10613 and JSA10663 previously to mitigate attacks and exploits ... KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories ...
Article Id: JSA10711

**2017-04 Security Bulletin: Junos: Multiple vulnerabilities in NTP [VU#633847]**  2023-0
In some cases, a Maintenance Release is not planned to be available in an appropriate ... Severity Assessment:Information for how Juniper Networks uses CVSS can be found at KB 16446 "Common ...
Article Id: JSA10776

**2021-04 Security Bulletin: Junos OS and Junos OS Evolved: Multiple NTP vulnerabilities resolved.**  2023-0
mask <mask_addr> noquery commit Note 1: With the above configuration all masked source addresses (source_address & mask ... T issue is being tracked as PR 1269141, 1446493 and 1446497 .
Article Id: JSA11171

**2023-04 Security Bulletin: Junos OS: QFX10000 Series, PTX1000 Series: The dcpfe process will crash when a malformed ethernet frame is received (CVE-2023-1697)**  2023-0
Title:2023-04 Security Bulletin: Junos OS: QFX10000 Series, PTX1000 Series: The dcpfe process will ... Affected platforms: PTX10 Series, QFX10000 Series.Severity Level:MediumCVSS Score:6.5 ( ...
Article Id: JSA70612

**2023-04 Security Bulletin: Junos OS: ACX Series: IPv6 firewall filter is not installed in PFE when "from next-header ah" is used (CVE-2023-28961)**  2023-0
This issue was seen during production usage. ... 2023-04-12: Initial Publication. Related Information:KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication ...
Article Id: JSA70586

**2023-04 Security Bulletin: Junos OS: Multiple vulnerabilities in J-Web**  2023-04-12
Title:2023-04 Security Bulletin: Junos OS: Multiple vulnerabilities in J-WebArticle ID:JSA70587Product ... By chaining exploitation of these vulnerabilities, an unauthenticated network-based ...
Article Id: JSA70587

## 2023-01 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 22.3R1 release

**Article ID** JSA70185  **Created** 2023-01-11  **Last Updated** 2023-05-22

Print  Report a Security Vulnerability

**Product Affected**

These issues affect all versions of Junos Space.

| Severity | Severity Assessment (CVSS) Score |
|---|---|
| Critical | 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U /C:H/I:H/A:H) |

**Problem**

Multiple vulnerabilities have been resolved in the Junos Space 22.3R1 release by updating third party software included with Junos Space or by fixing vulnerabilities found during external security research.

These issues affect Juniper Networks Junos Space versions prior to 22.3R1.

Juniper SIRT is not aware of any malicious exploitation of these vulnerabilities.

These issue were discovered during external security research.

Important security issues resolved include:

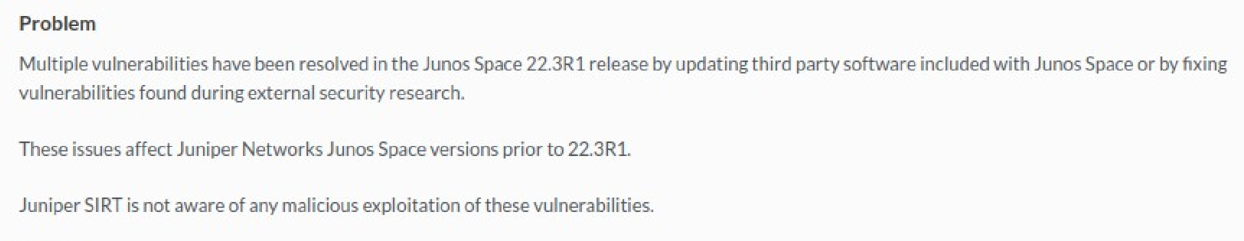
| CVE | CVSS | Summary |
|---|---|---|
| CVE-2022-29154 | 7.4 (CVSS:3.1/AV:N /AC:H/PR:N /UI:N/S:U /C:N/I:H/A:H) | An issue was discovered in rsync before 3.2.5 that allows malicious remote servers to write arbitrary files inside the directories of connecting peers. The server chooses which files/directories are sent to the client. However, the rsync client performs insufficient validation of file names. A malicious rsync server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the rsync client target directory and subdirectories (for example, overwrite the .ssh/authorized_keys file). |
| CVE-2022-2526 | 9.8 (CVSS:3.1/AV:N /AC:L/PR:N /UI:N/S:U /C:H/I:H/A:H) | A use-after-free vulnerability was found in systemd. This issue occurs due to the on_stream_io() function and dns_stream_complete() function in 'resolved-dns-stream.c' not incrementing the reference counting for the DnsStream object. Therefore, other functions and callbacks called can dereference the DNSStream object, causing the use-after-free when the reference is still used later. |
| CVE-2022-21541 | 5.9 (CVSS:3.1/AV:N /AC:H/PR:N /UI:N/S:U /C:N/I:H/A:N) | Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). |

People also viewed

- 2015-10 Out of Cycle Security Bulletin: NTP.org announcement of multiple vulnerabilities.
- 2017-04 Security Bulletin: Junos: Multiple vulnerabilities in NTP [VU#633847]
- 2021-04 Security Bulletin: Junos OS and Junos OS Evolved: Multiple NTP vulnerabilities resolved.
- 2023-04 Security Bulletin: Junos OS: ACX Series: IPv6 firewall filter is not installed in PFE when "from next-header ah" is used (CVE-2023-28961)
- 2023-04 Security Bulletin: Junos OS: QFX10000 Series, PTX1000 Series: The dcpfe process will crash when a malformed ethernet frame is received (CVE-2023-1697)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: If malformed IPv6 router advertisements are received, memory corruption will occur which causes an rpd crash (CVE-2023-28981)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: In a BGP rib sharding scenario an rpd crash will happen shortly after a specific CLI command is issued (CVE-2023-28980)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: In a BGP rib sharding scenario when a route is frequently updated an rpd memory leak will occur (CVE-2023-28982)
- 2023-04 Security Bulletin: Junos OS: Multiple vulnerabilities in J-Web
- 2023-01 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 22.3R1 release

https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&f:ctype=[Security%20Advisories]

# affected version の記述はそれぞれ

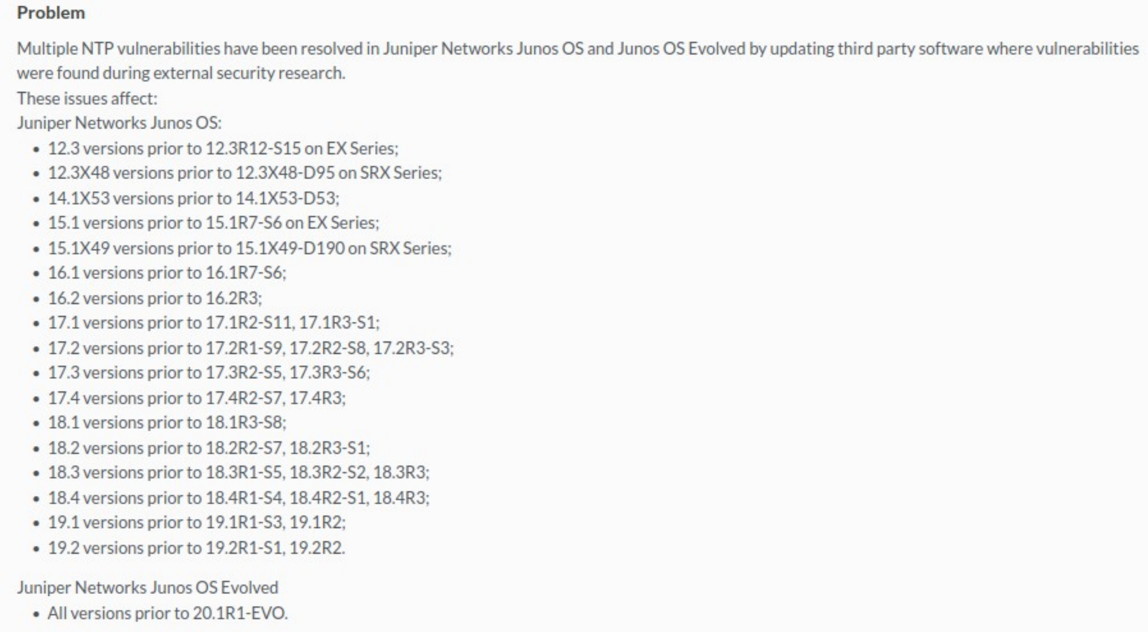


**Problem**

Multiple vulnerabilities have been resolved in the Junos Space 22.3R1 release by updating third party software included with Junos Space or by fixing vulnerabilities found during external security research.

These issues affect Juniper Networks Junos Space versions prior to 22.3R1.

Juniper SIRT is not aware of any malicious exploitation of these vulnerabilities.



**Problem**

Multiple NTP vulnerabilities have been resolved in Juniper Networks Junos OS and Junos OS Evolved by updating third party software where vulnerabilities were found during external security research.
These issues affect:
Juniper Networks Junos OS:

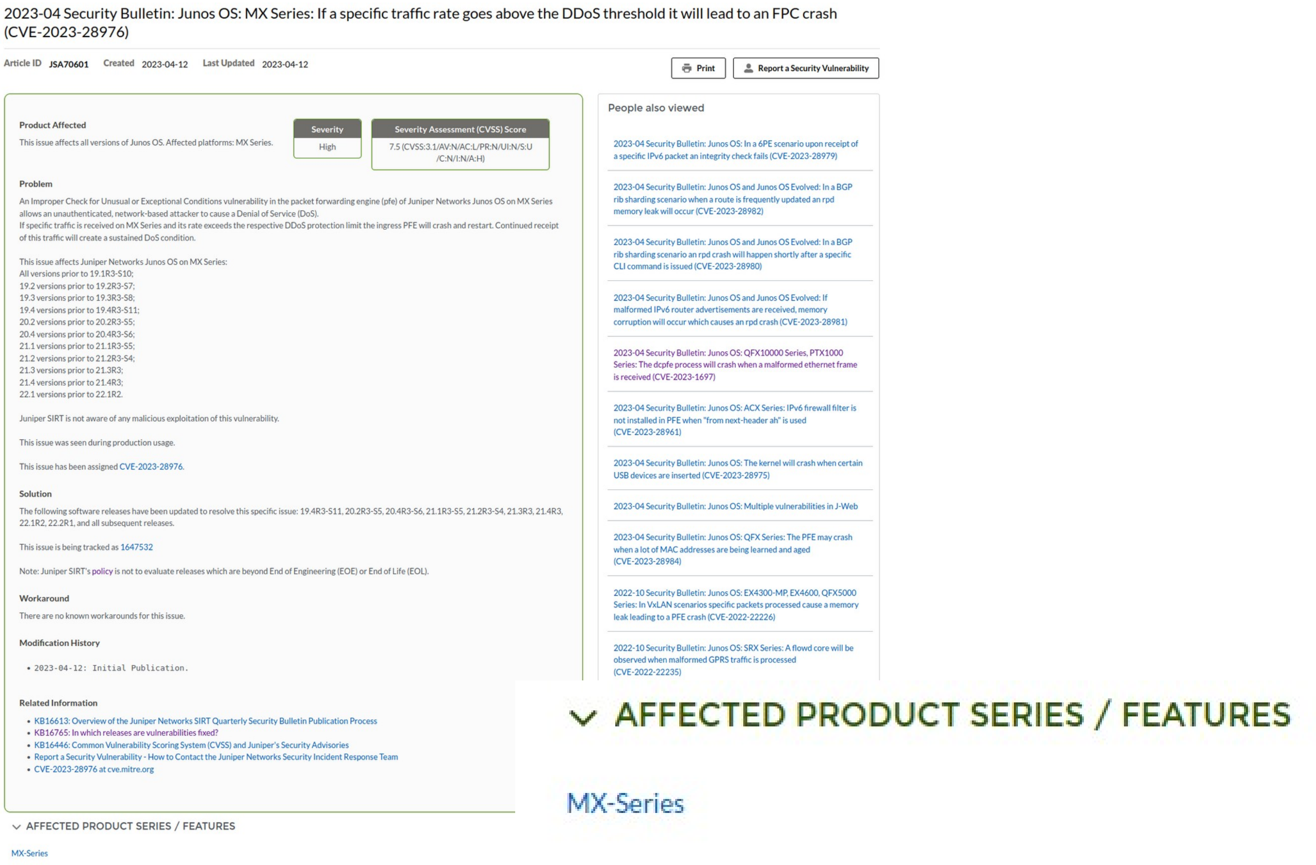
- 12.3 versions prior to 12.3R12-S15 on EX Series;
- 12.3X48 versions prior to 12.3X48-D95 on SRX Series;
- 14.1X53 versions prior to 14.1X53-D53;
- 15.1 versions prior to 15.1R7-S6 on EX Series;
- 15.1X49 versions prior to 15.1X49-D190 on SRX Series;
- 16.1 versions prior to 16.1R7-S6;
- 16.2 versions prior to 16.2R3;
- 17.1 versions prior to 17.1R2-S11, 17.1R3-S1;
- 17.2 versions prior to 17.2R1-S9, 17.2R2-S8, 17.2R3-S3;
- 17.3 versions prior to 17.3R2-S5, 17.3R3-S6;
- 17.4 versions prior to 17.4R2-S7, 17.4R3;
- 18.1 versions prior to 18.1R3-S8;
- 18.2 versions prior to 18.2R2-S7, 18.2R3-S1;
- 18.3 versions prior to 18.3R1-S5, 18.3R2-S2, 18.3R3;
- 18.4 versions prior to 18.4R1-S4, 18.4R2-S1, 18.4R3;
- 19.1 versions prior to 19.1R1-S3, 19.1R2;
- 19.2 versions prior to 19.2R1-S1, 19.2R2.

Juniper Networks Junos OS Evolved

- All versions prior to 20.1R1-EVO.

[1] https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-22-3R1-release?language=en_US
[2] https://supportportal.juniper.net/s/article/2021-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-NTP-vulnerabilities-resolved?language=en_US

# affected product でシリーズ名しか書いておらず、対象製品を別に調べる必要がある



2023-04 Security Bulletin: Junos OS: MX Series: If a specific traffic rate goes above the DDoS threshold it will lead to an FPC crash (CVE-2023-28976)

Article ID JSA70601 Created 2023-04-12 Last Updated 2023-04-12

**Product Affected**

This issue affects all versions of Junos OS. Affected platforms: MX Series.

| Severity | Severity Assessment (CVSS) Score |
|---|---|
| High | 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) |

**Problem**

An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS).
If specific traffic is received on MX Series and its rate exceeds the respective DDoS protection limit the ingress PFE will crash and restart. Continued receipt of this traffic will create a sustained DoS condition.

This issue affects Juniper Networks Junos OS on MX Series:
All versions prior to 19.1R3-S10;
19.2 versions prior to 19.2R3-S7;
19.3 versions prior to 19.3R3-S8;
19.4 versions prior to 19.4R3-S11;
20.2 versions prior to 20.2R3-S5;
20.4 versions prior to 20.4R3-S6;
21.1 versions prior to 21.1R3-S5;
21.2 versions prior to 21.2R3-S4;
21.3 versions prior to 21.3R3;
21.4 versions prior to 21.4R3;
22.1 versions prior to 22.1R2.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

This issue was seen during production usage.

This issue has been assigned CVE-2023-28976.

**Solution**

The following software releases have been updated to resolve this specific issue: 19.4R3-S11, 20.2R3-S5, 20.4R3-S6, 21.1R3-S5, 21.2R3-S4, 21.3R3, 21.4R3, 22.1R2, 22.2R1, and all subsequent releases.

This issue is being tracked as 1647532

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

**Workaround**

There are no known workarounds for this issue.

**Modification History**

- `2023-04-12: Initial Publication.`

**Related Information**

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- CVE-2023-28976 at cve.mitre.org

AFFECTED PRODUCT SERIES / FEATURES

MX-Series

People also viewed

- 2023-04 Security Bulletin: Junos OS: In a 6PE scenario upon receipt of a specific IPv6 packet an integrity check fails (CVE-2023-28979)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: In a BGP rib sharding scenario when a route is frequently updated an rpd memory leak will occur (CVE-2023-28982)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: In a BGP rib sharding scenario an rpd crash will happen shortly after a specific CLI command is issued (CVE-2023-28980)
- 2023-04 Security Bulletin: Junos OS and Junos OS Evolved: If malformed IPv6 router advertisements are received, memory corruption will occur which causes an rpd crash (CVE-2023-28981)
- 2023-04 Security Bulletin: Junos OS: QFX10000 Series, PTX1000 Series: The dcpfe process will crash when a malformed ethernet frame is received (CVE-2023-1697)
- 2023-04 Security Bulletin: Junos OS: ACX Series: IPv6 firewall filter is not installed in PFE when "from next-header ah" is used (CVE-2023-28961)
- 2023-04 Security Bulletin: Junos OS: The kernel will crash when certain USB devices are inserted (CVE-2023-28975)
- 2023-04 Security Bulletin: Junos OS: Multiple vulnerabilities in J-Web
- 2023-04 Security Bulletin: Junos OS: QFX Series: The PFE may crash when a lot of MAC addresses are being learned and aged (CVE-2023-28984)
- 2022-10 Security Bulletin: Junos OS: EX4300-MP, EX4600, QFX5000 Series: In VxLAN scenarios specific packets processed cause a memory leak leading to a PFE crash (CVE-2022-22226)
- 2022-10 Security Bulletin: Junos OS: SRX Series: A flowd core will be observed when malformed GPRS traffic is processed (CVE-2022-22235)

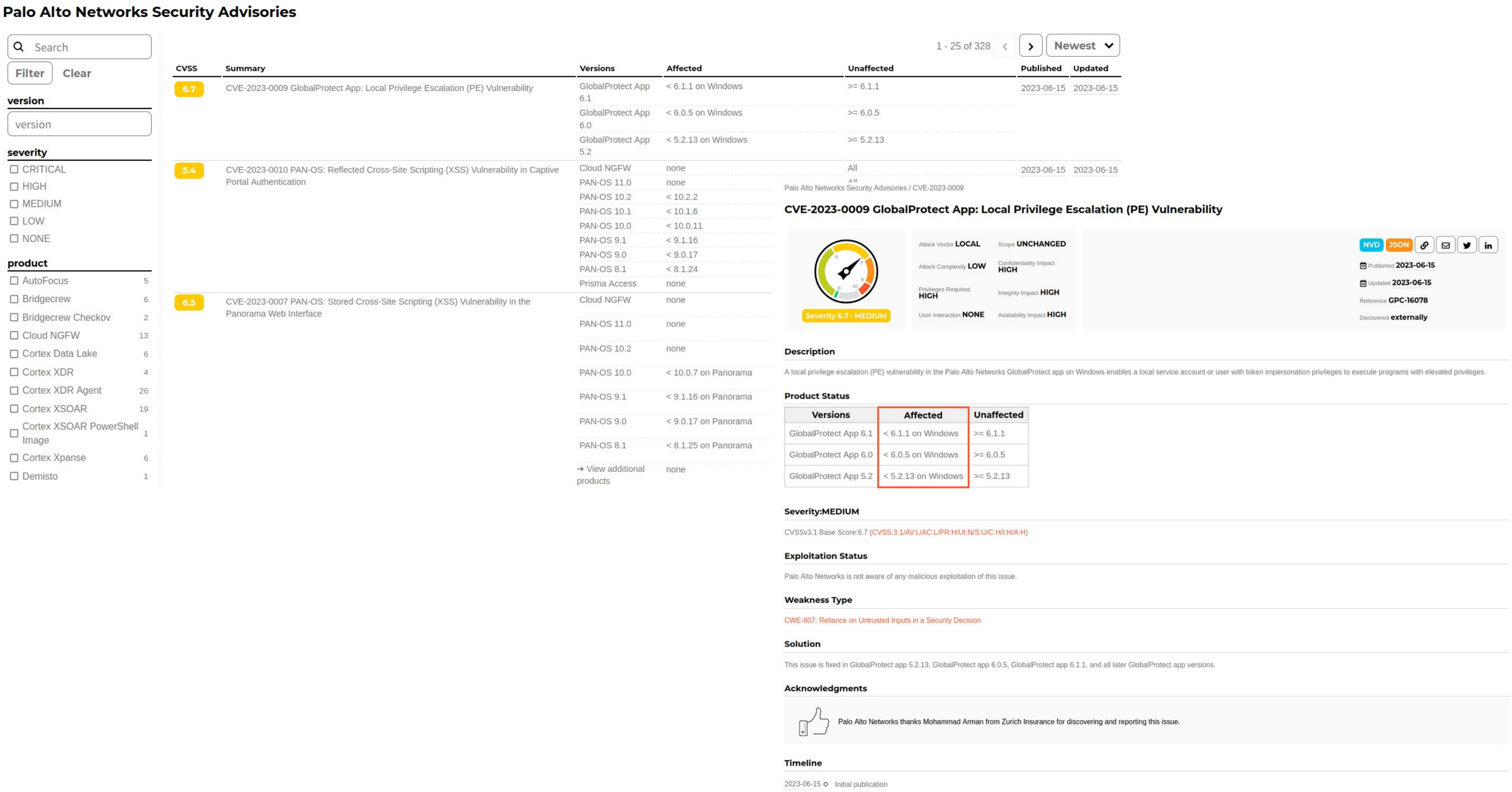
AFFECTED PRODUCT SERIES / FEATURES

MX-Series

https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-MX-Series-If-a-specific-traffic-rate-goes-above-the-DDoS-threshold-it-will-lead-to-an-FPC-crash-CVE-2023-28976?language=en_US

# Palo Alto Networks

# 総アドバイザリ数：328 /  ページネーション  / Web, MITRE CVE 4.0 JSON



## Palo Alto Networks Security Advisories

Search

Filter   Clear

**version**

version

**severity**

- ☐ CRITICAL
- ☐ HIGH
- ☐ MEDIUM
- ☐ LOW
- ☐ NONE

**product**

| | |
|---|---|
| ☐ AutoFocus | 5 |
| ☐ Bridgecrew | 6 |
| ☐ Bridgecrew Checkov | 2 |
| ☐ Cloud NGFW | 13 |
| ☐ Cortex Data Lake | 6 |
| ☐ Cortex XDR | 4 |
| ☐ Cortex XDR Agent | 26 |
| ☐ Cortex XSOAR | 19 |
| ☐ Cortex XSOAR PowerShell Image | 1 |
| ☐ Cortex Xpanse | 6 |
| ☐ Demisto | 1 |

1 - 25 of 328 ‹ › Newest

| CVSS | Summary | Versions | Affected | Unaffected | Published | Updated |
|---|---|---|---|---|---|---|
| 6.7 | CVE-2023-0009 GlobalProtect App: Local Privilege Escalation (PE) Vulnerability | GlobalProtect App 6.1 | < 6.1.1 on Windows | >= 6.1.1 | 2023-06-15 | 2023-06-15 |
| | | GlobalProtect App 6.0 | < 6.0.5 on Windows | >= 6.0.5 | | |
| | | GlobalProtect App 5.2 | < 5.2.13 on Windows | >= 5.2.13 | | |
| 5.4 | CVE-2023-0010 PAN-OS: Reflected Cross-Site Scripting (XSS) Vulnerability in Captive Portal Authentication | Cloud NGFW | none | All | 2023-06-15 | 2023-06-15 |
| | | PAN-OS 11.0 | none | All | | |
| | | PAN-OS 10.2 | < 10.2.2 | | | |
| | | PAN-OS 10.1 | < 10.1.6 | | | |
| | | PAN-OS 10.0 | < 10.0.11 | | | |
| | | PAN-OS 9.1 | < 9.1.16 | | | |
| | | PAN-OS 9.0 | < 9.0.17 | | | |
| | | PAN-OS 8.1 | < 8.1.24 | | | |
| | | Prisma Access | none | | | |
| 6.5 | CVE-2023-0007 PAN-OS: Stored Cross-Site Scripting (XSS) Vulnerability in the Panorama Web Interface | Cloud NGFW | none | | | |
| | | PAN-OS 11.0 | none | | | |
| | | PAN-OS 10.2 | none | | | |
| | | PAN-OS 10.0 | < 10.0.7 on Panorama | | | |
| | | PAN-OS 9.1 | < 9.1.16 on Panorama | | | |
| | | PAN-OS 9.0 | < 9.0.17 on Panorama | | | |
| | | PAN-OS 8.1 | < 8.1.25 on Panorama | | | |
| | | → View additional products | none | | | |

Palo Alto Networks Security Advisories / CVE-2023-0009

### CVE-2023-0009 GlobalProtect App: Local Privilege Escalation (PE) Vulnerability

Severity 6.7 · MEDIUM

| | |
|---|---|
| Attack Vector **LOCAL** | Scope **UNCHANGED** |
| Attack Complexity **LOW** | Confidentiality Impact **HIGH** |
| Privileges Required **HIGH** | Integrity Impact **HIGH** |
| User Interaction **NONE** | Availability Impact **HIGH** |

NVD JSON

Published **2023-06-15**

Updated **2023-06-15**

Reference **GPC-16078**

Discovered **externally**

**Description**

A local privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows enables a local service account or user with token impersonation privileges to execute programs with elevated privileges.

**Product Status**

| Versions | Affected | Unaffected |
|---|---|---|
| GlobalProtect App 6.1 | < 6.1.1 on Windows | >= 6.1.1 |
| GlobalProtect App 6.0 | < 6.0.5 on Windows | >= 6.0.5 |
| GlobalProtect App 5.2 | < 5.2.13 on Windows | >= 5.2.13 |

**Severity:MEDIUM**

CVSSv3.1 Base Score:6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

**Exploitation Status**

Palo Alto Networks is not aware of any malicious exploitation of this issue.

**Weakness Type**

CWE-807: Reliance on Untrusted Inputs in a Security Decision

**Solution**

This issue is fixed in GlobalProtect app 5.2.13, GlobalProtect app 6.0.5, GlobalProtect app 6.1.1, and all later GlobalProtect app versions.

**Acknowledgments**

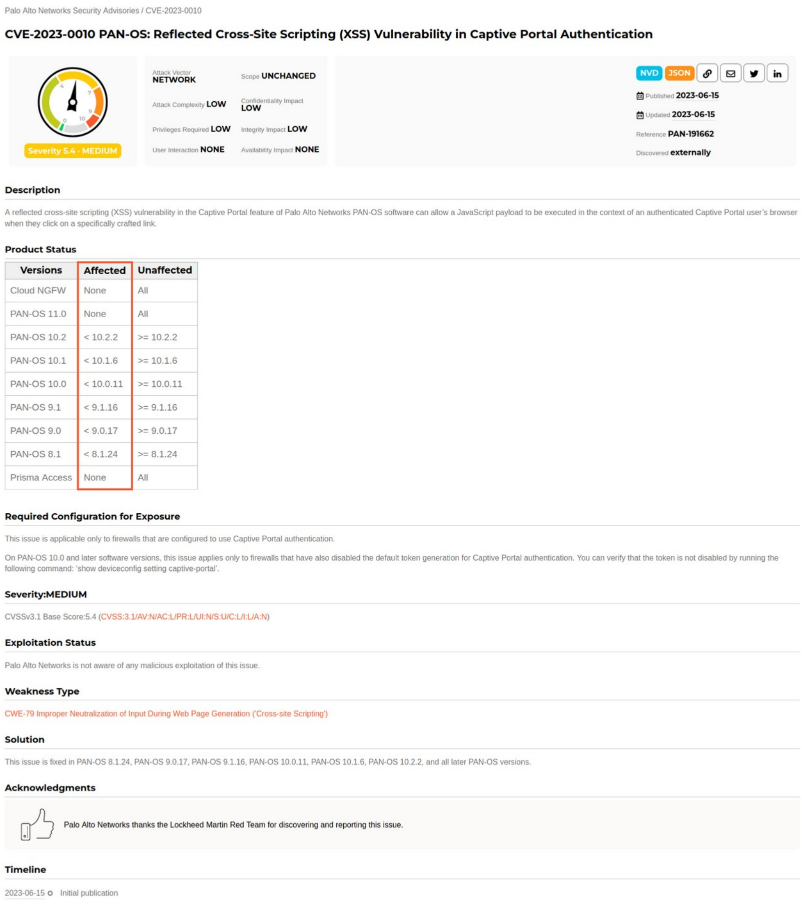
Palo Alto Networks thanks Mohammad Arman from Zurich Insurance for discovering and reporting this issue.

**Timeline**

2023-06-15 ○ Initial publication

https://security.paloaltonetworks.com/

# MITRE CVE 4.0 JSON で web 版と同等の情報にアクセスできる



Palo Alto Networks Security Advisories / CVE-2023-0010

**CVE-2023-0010 PAN-OS: Reflected Cross-Site Scripting (XSS) Vulnerability in Captive Portal Authentication**

Severity 5.4 · MEDIUM

| | |
|---|---|
| Attack Vector **NETWORK** | Scope **UNCHANGED** |
| Attack Complexity **LOW** | Confidentiality Impact **LOW** |
| Privileges Required **LOW** | Integrity Impact **LOW** |
| User Interaction **NONE** | Availability Impact **NONE** |

Published **2023-06-15**
Updated **2023-06-15**
Reference **PAN-191662**
Discovered **externally**

**Description**

A reflected cross-site scripting (XSS) vulnerability in the Captive Portal feature of Palo Alto Networks PAN-OS software can allow a JavaScript payload to be executed in the context of an authenticated Captive Portal user's browser when they click on a specifically crafted link.

**Product Status**

| Versions | Affected | Unaffected |
|---|---|---|
| Cloud NGFW | None | All |
| PAN-OS 11.0 | None | All |
| PAN-OS 10.2 | < 10.2.2 | >= 10.2.2 |
| PAN-OS 10.1 | < 10.1.6 | >= 10.1.6 |
| PAN-OS 10.0 | < 10.0.11 | >= 10.0.11 |
| PAN-OS 9.1 | < 9.1.16 | >= 9.1.16 |
| PAN-OS 9.0 | < 9.0.17 | >= 9.0.17 |
| PAN-OS 8.1 | < 8.1.24 | >= 8.1.24 |
| Prisma Access | None | All |

**Required Configuration for Exposure**

This issue is applicable only to firewalls that are configured to use Captive Portal authentication.

On PAN-OS 10.0 and later software versions, this issue applies only to firewalls that have also disabled the default token generation for Captive Portal authentication. You can verify that the token is not disabled by running the following command: 'show deviceconfig setting captive-portal'.

**Severity:MEDIUM**

CVSSv3.1 Base Score:5.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

**Exploitation Status**

Palo Alto Networks is not aware of any malicious exploitation of this issue.

**Weakness Type**

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Solution**

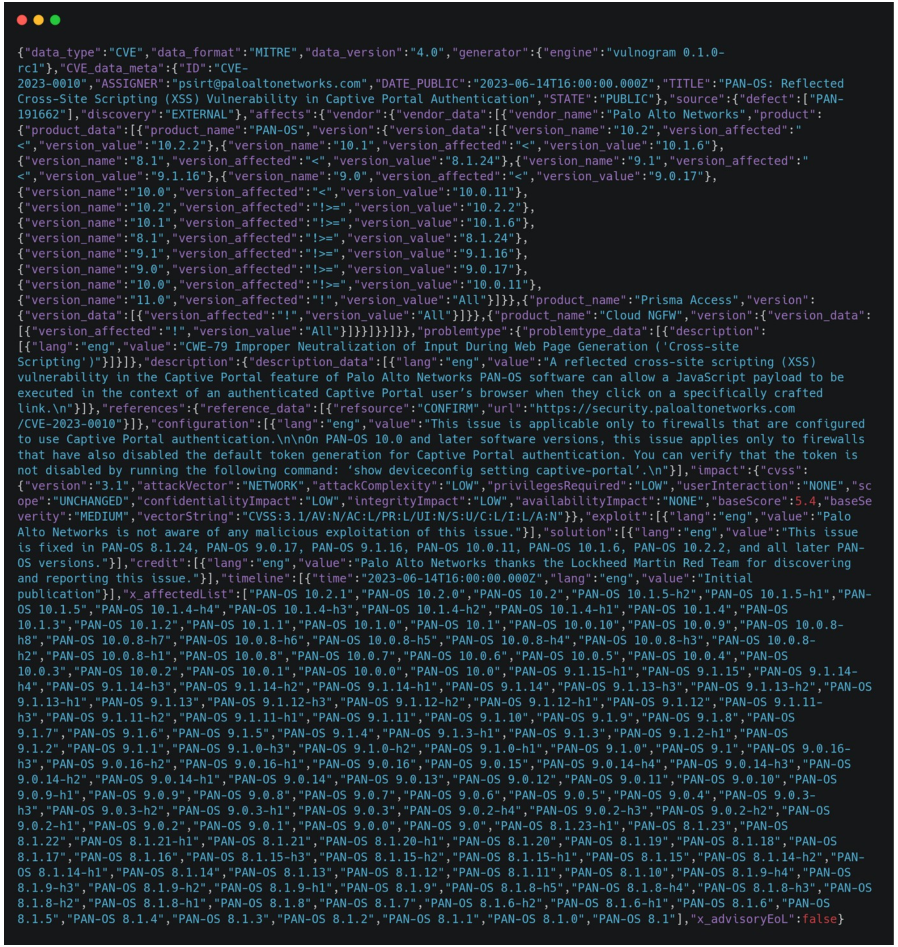
This issue is fixed in PAN-OS 8.1.24, PAN-OS 9.0.17, PAN-OS 9.1.16, PAN-OS 10.0.11, PAN-OS 10.1.6, PAN-OS 10.2.2, and all later PAN-OS versions.

**Acknowledgments**

Palo Alto Networks thanks the Lockheed Martin Red Team for discovering and reporting this issue.

**Timeline**

2023-06-15 ○ Initial publication

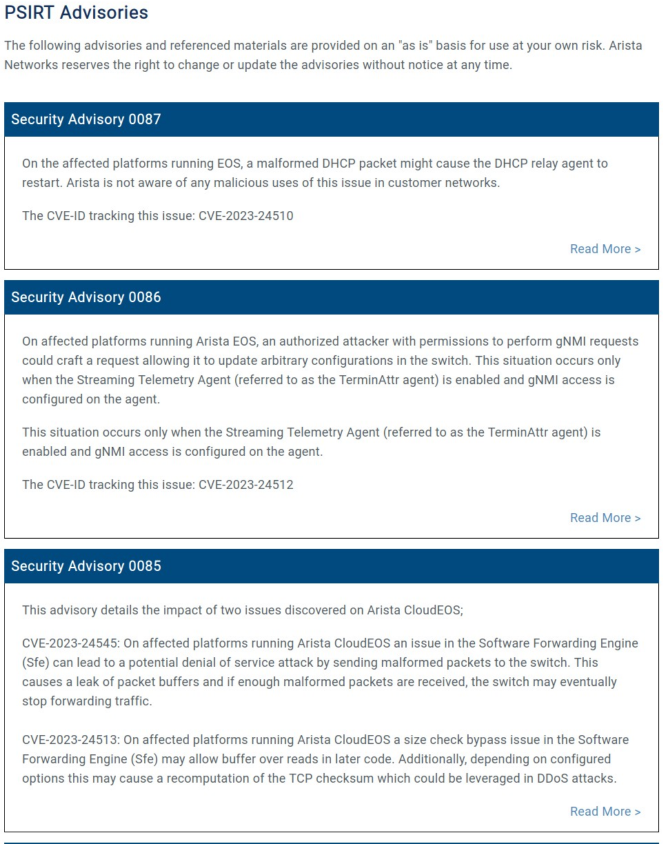


```
{"data_type":"CVE","data_format":"MITRE","data_version":"4.0","generator":{"engine":"vulnogram 0.1.0-
rc1"},"CVE_data_meta":{"ID":"CVE-
2023-0010","ASSIGNER":"psirt@paloaltonetworks.com","DATE_PUBLIC":"2023-06-14T16:00:00.000Z","TITLE":"PAN-OS: Reflected
Cross-Site Scripting (XSS) Vulnerability in Captive Portal Authentication","STATE":"PUBLIC"},"source":{"defect":["PAN-
191662"],"discovery":"EXTERNAL"},"affects":{"vendor":{"vendor_data":[{"vendor_name":"Palo Alto Networks","product":
{"product_data":[{"product_name":"PAN-OS","version":{"version_data":[{"version_name":"10.2","version_affected":"
<","version_value":"10.2.2"},{"version_name":"10.1","version_affected":"<","version_value":"10.1.6"},
{"version_name":"8.1","version_affected":"<","version_value":"8.1.24"},{"version_name":"9.1","version_affected":"
<","version_value":"9.1.16"},{"version_name":"9.0","version_affected":"<","version_value":"9.0.17"},
{"version_name":"10.0","version_affected":"<","version_value":"10.0.11"},
{"version_name":"10.2","version_affected":"!>=","version_value":"10.2.2"},
{"version_name":"10.1","version_affected":"!>=","version_value":"10.1.6"},
{"version_name":"8.1","version_affected":"!>=","version_value":"8.1.24"},
{"version_name":"9.1","version_affected":"!>=","version_value":"9.1.16"},
{"version_name":"9.0","version_affected":"!>=","version_value":"9.0.17"},
{"version_name":"10.0","version_affected":"!>=","version_value":"10.0.11"},
{"version_name":"11.0","version_affected":"!","version_value":"All"}]}},{"product_name":"Prisma Access","version":
{"version_data":[{"version_affected":"!","version_value":"All"}]}},{"product_name":"Cloud NGFW","version":{"version_data":
[{"version_affected":"!","version_value":"All"}]}}]}}]}},"problemtype":{"problemtype_data":[{"description":
[{"lang":"eng","value":"CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site
Scripting')"}]}]},"description":{"description_data":[{"lang":"eng","value":"A reflected cross-site scripting (XSS)
vulnerability in the Captive Portal feature of Palo Alto Networks PAN-OS software can allow a JavaScript payload to be
executed in the context of an authenticated Captive Portal user’s browser when they click on a specifically crafted
link.\n"}]},"references":{"reference_data":[{"refsource":"CONFIRM","url":"https://security.paloaltonetworks.com
/CVE-2023-0010"}]},"configuration":[{"lang":"eng","value":"This issue is applicable only to firewalls that are configured
to use Captive Portal authentication.\n\nOn PAN-OS 10.0 and later software versions, this issue applies only to firewalls
that have also disabled the default token generation for Captive Portal authentication. You can verify that the token is
not disabled by running the following command: ‘show deviceconfig setting captive-portal’.\n"}],"impact":{"cvss":
{"version":"3.1","attackVector":"NETWORK","attackComplexity":"LOW","privilegesRequired":"LOW","userInteraction":"NONE","sc
ope":"UNCHANGED","confidentialityImpact":"LOW","integrityImpact":"LOW","availabilityImpact":"NONE","baseScore":5.4,"baseSe
verity":"MEDIUM","vectorString":"CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N"}},"exploit":[{"lang":"eng","value":"Palo
Alto Networks is not aware of any malicious exploitation of this issue."}],"solution":[{"lang":"eng","value":"This issue
is fixed in PAN-OS 8.1.24, PAN-OS 9.0.17, PAN-OS 9.1.16, PAN-OS 10.0.11, PAN-OS 10.1.6, PAN-OS 10.2.2, and all later PAN-
OS versions."}],"credit":[{"lang":"eng","value":"Palo Alto Networks thanks the Lockheed Martin Red Team for discovering
and reporting this issue."}],"timeline":[{"time":"2023-06-14T16:00:00.000Z","lang":"eng","value":"Initial
publication"}],"x_affectedList":["PAN-OS 10.2.1","PAN-OS 10.2.0","PAN-OS 10.2","PAN-OS 10.1.5-h2","PAN-OS 10.1.5-h1","PAN-
OS 10.1.5","PAN-OS 10.1.4-h4","PAN-OS 10.1.4-h3","PAN-OS 10.1.4-h2","PAN-OS 10.1.4-h1","PAN-OS 10.1.4","PAN-OS
10.1.3","PAN-OS 10.1.2","PAN-OS 10.1.1","PAN-OS 10.1.0","PAN-OS 10.1","PAN-OS 10.0.10","PAN-OS 10.0.9","PAN-OS 10.0.8-
h8","PAN-OS 10.0.8-h7","PAN-OS 10.0.8-h6","PAN-OS 10.0.8-h5","PAN-OS 10.0.8-h4","PAN-OS 10.0.8-h3","PAN-OS 10.0.8-
h2","PAN-OS 10.0.8-h1","PAN-OS 10.0.8","PAN-OS 10.0.7","PAN-OS 10.0.6","PAN-OS 10.0.5","PAN-OS 10.0.4","PAN-OS
10.0.3","PAN-OS 10.0.2","PAN-OS 10.0.1","PAN-OS 10.0.0","PAN-OS 10.0","PAN-OS 9.1.15-h1","PAN-OS 9.1.15","PAN-OS 9.1.14-
h4","PAN-OS 9.1.14-h3","PAN-OS 9.1.14-h2","PAN-OS 9.1.14-h1","PAN-OS 9.1.14","PAN-OS 9.1.13-h3","PAN-OS 9.1.13-h2","PAN-OS
9.1.13-h1","PAN-OS 9.1.13","PAN-OS 9.1.12-h3","PAN-OS 9.1.12-h2","PAN-OS 9.1.12-h1","PAN-OS 9.1.12","PAN-OS 9.1.11-
h3","PAN-OS 9.1.11-h2","PAN-OS 9.1.11-h1","PAN-OS 9.1.11","PAN-OS 9.1.10","PAN-OS 9.1.9","PAN-OS 9.1.8","PAN-OS
9.1.7","PAN-OS 9.1.6","PAN-OS 9.1.5","PAN-OS 9.1.4","PAN-OS 9.1.3-h1","PAN-OS 9.1.3","PAN-OS 9.1.2-h1","PAN-OS
9.1.2","PAN-OS 9.1.1","PAN-OS 9.1.0-h3","PAN-OS 9.1.0-h2","PAN-OS 9.1.0-h1","PAN-OS 9.1.0","PAN-OS 9.1","PAN-OS 9.0.16-
h3","PAN-OS 9.0.16-h2","PAN-OS 9.0.16-h1","PAN-OS 9.0.16","PAN-OS 9.0.15","PAN-OS 9.0.14-h4","PAN-OS 9.0.14-h3","PAN-OS
9.0.14-h2","PAN-OS 9.0.14-h1","PAN-OS 9.0.14","PAN-OS 9.0.13","PAN-OS 9.0.12","PAN-OS 9.0.11","PAN-OS 9.0.10","PAN-OS
9.0.9-h1","PAN-OS 9.0.9","PAN-OS 9.0.8","PAN-OS 9.0.7","PAN-OS 9.0.6","PAN-OS 9.0.5","PAN-OS 9.0.4","PAN-OS 9.0.3-
h3","PAN-OS 9.0.3-h2","PAN-OS 9.0.3-h1","PAN-OS 9.0.3","PAN-OS 9.0.2-h4","PAN-OS 9.0.2-h3","PAN-OS 9.0.2-h2","PAN-OS
9.0.2-h1","PAN-OS 9.0.2","PAN-OS 9.0.1","PAN-OS 9.0.0","PAN-OS 9.0","PAN-OS 8.1.23-h1","PAN-OS 8.1.23","PAN-OS
8.1.22","PAN-OS 8.1.21-h1","PAN-OS 8.1.21","PAN-OS 8.1.20-h1","PAN-OS 8.1.20","PAN-OS 8.1.19","PAN-OS 8.1.18","PAN-OS
8.1.17","PAN-OS 8.1.16","PAN-OS 8.1.15-h3","PAN-OS 8.1.15-h2","PAN-OS 8.1.15-h1","PAN-OS 8.1.15","PAN-OS 8.1.14-h2","PAN-
OS 8.1.14-h1","PAN-OS 8.1.14","PAN-OS 8.1.13","PAN-OS 8.1.12","PAN-OS 8.1.11","PAN-OS 8.1.10","PAN-OS 8.1.9-h4","PAN-OS
8.1.9-h3","PAN-OS 8.1.9-h2","PAN-OS 8.1.9-h1","PAN-OS 8.1.9","PAN-OS 8.1.8-h5","PAN-OS 8.1.8-h4","PAN-OS 8.1.8-h3","PAN-OS
8.1.8-h2","PAN-OS 8.1.8-h1","PAN-OS 8.1.8","PAN-OS 8.1.7","PAN-OS 8.1.6-h2","PAN-OS 8.1.6-h1","PAN-OS 8.1.6","PAN-OS
8.1.5","PAN-OS 8.1.4","PAN-OS 8.1.3","PAN-OS 8.1.2","PAN-OS 8.1.1","PAN-OS 8.1.0","PAN-OS 8.1"],"x_advisoryEoL":false}
```

[1] https://security.paloaltonetworks.com/CVE-2023-0010
[2] https://security.paloaltonetworks.com/json/CVE-2023-0010

# Arista Network

# 総アドバイザリ数: 87 / ページネーション / Web, PDF, CSAF



## PSIRT Advisories

The following advisories and referenced materials are provided on an "as is" basis for use at your own risk. Arista Networks reserves the right to change or update the advisories without notice at any time.

### Security Advisory 0087

On the affected platforms running EOS, a malformed DHCP packet might cause the DHCP relay agent to restart. Arista is not aware of any malicious uses of this issue in customer networks.

The CVE-ID tracking this issue: CVE-2023-24510

Read More >

### Security Advisory 0086

On affected platforms running Arista EOS, an authorized attacker with permissions to perform gNMI requests could craft a request allowing it to update arbitrary configurations in the switch. This situation occurs only when the Streaming Telemetry Agent (referred to as the TerminAttr agent) is enabled and gNMI access is configured on the agent.

This situation occurs only when the Streaming Telemetry Agent (referred to as the TerminAttr agent) is enabled and gNMI access is configured on the agent.

The CVE-ID tracking this issue: CVE-2023-24512

Read More >

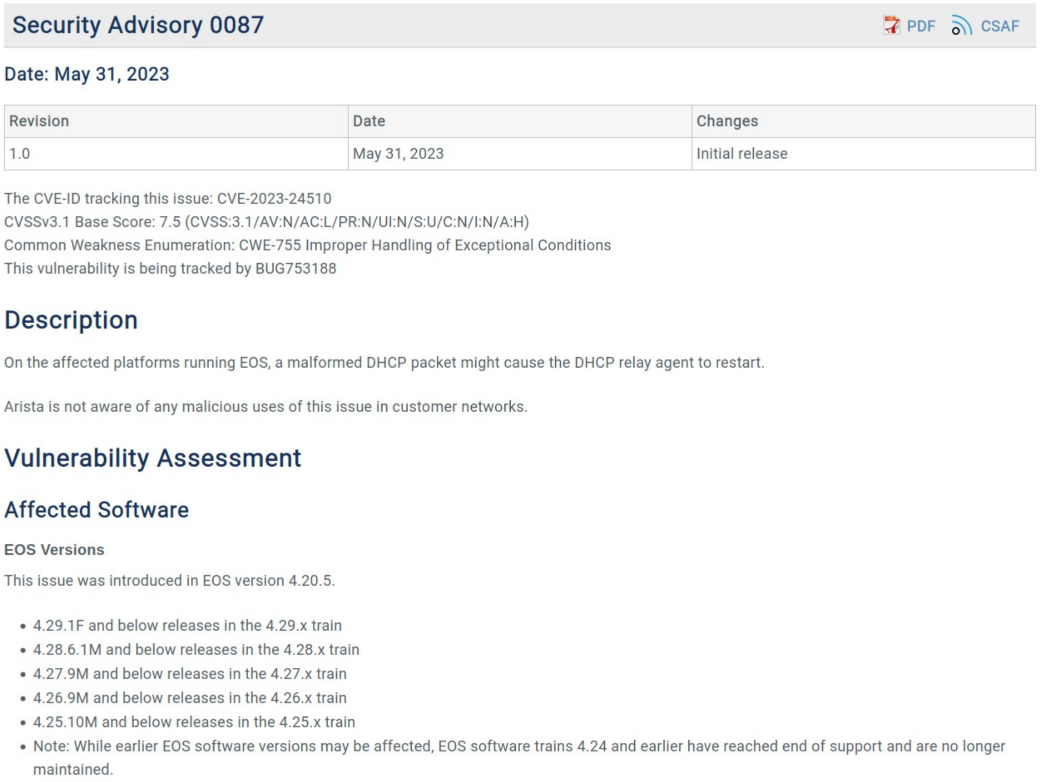
### Security Advisory 0085

This advisory details the impact of two issues discovered on Arista CloudEOS;

CVE-2023-24545: On affected platforms running Arista CloudEOS an issue in the Software Forwarding Engine (Sfe) can lead to a potential denial of service attack by sending malformed packets to the switch. This causes a leak of packet buffers and if enough malformed packets are received, the switch may eventually stop forwarding traffic.

CVE-2023-24513: On affected platforms running Arista CloudEOS a size check bypass issue in the Software Forwarding Engine (Sfe) may allow buffer over reads in later code. Additionally, depending on configured options this may cause a recomputation of the TCP checksum which could be leveraged in DDoS attacks.

Read More >



## Security Advisory 0087

**Date: May 31, 2023**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | May 31, 2023 | Initial release |

The CVE-ID tracking this issue: CVE-2023-24510
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Common Weakness Enumeration: CWE-755 Improper Handling of Exceptional Conditions
This vulnerability is being tracked by BUG753188

## Description

On the affected platforms running EOS, a malformed DHCP packet might cause the DHCP relay agent to restart.

Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

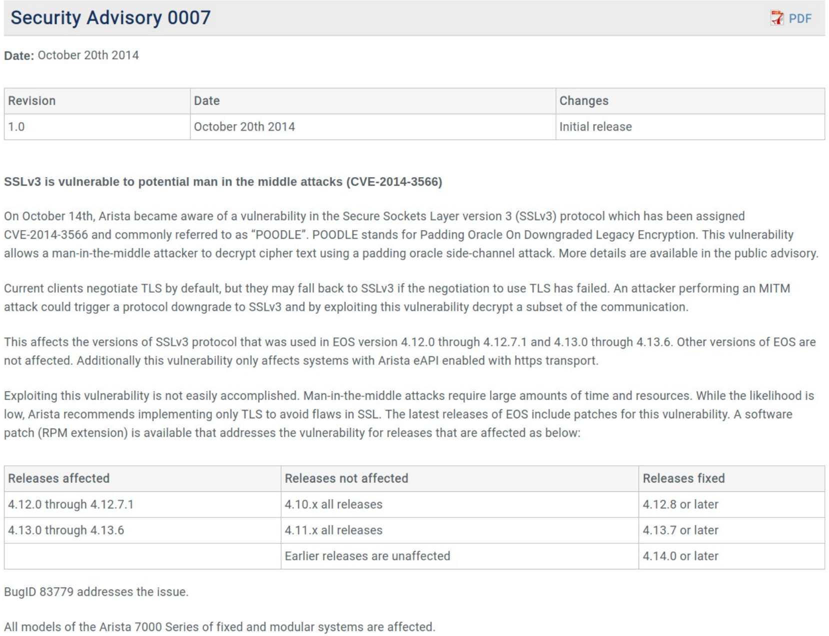
**EOS Versions**

This issue was introduced in EOS version 4.20.5.

- 4.29.1F and below releases in the 4.29.x train
- 4.28.6.1M and below releases in the 4.28.x train
- 4.27.9M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train
- 4.25.10M and below releases in the 4.25.x train
- Note: While earlier EOS software versions may be affected, EOS software trains 4.24 and earlier have reached end of support and are no longer maintained.

https://www.arista.com/en/support/advisories-notices

# Web 版では Affected などが自由文法で書かれている



## Security Advisory 0007

PDF

**Date:** October 20th 2014

| Revision | Date | Changes |
|---|---|---|
| 1.0 | October 20th 2014 | Initial release |

**SSLv3 is vulnerable to potential man in the middle attacks (CVE-2014-3566)**

On October 14th, Arista became aware of a vulnerability in the Secure Sockets Layer version 3 (SSLv3) protocol which has been assigned CVE-2014-3566 and commonly referred to as "POODLE". POODLE stands for Padding Oracle On Downgraded Legacy Encryption. This vulnerability allows a man-in-the-middle attacker to decrypt cipher text using a padding oracle side-channel attack. More details are available in the public advisory.

Current clients negotiate TLS by default, but they may fall back to SSLv3 if the negotiation to use TLS has failed. An attacker performing an MITM attack could trigger a protocol downgrade to SSLv3 and by exploiting this vulnerability decrypt a subset of the communication.

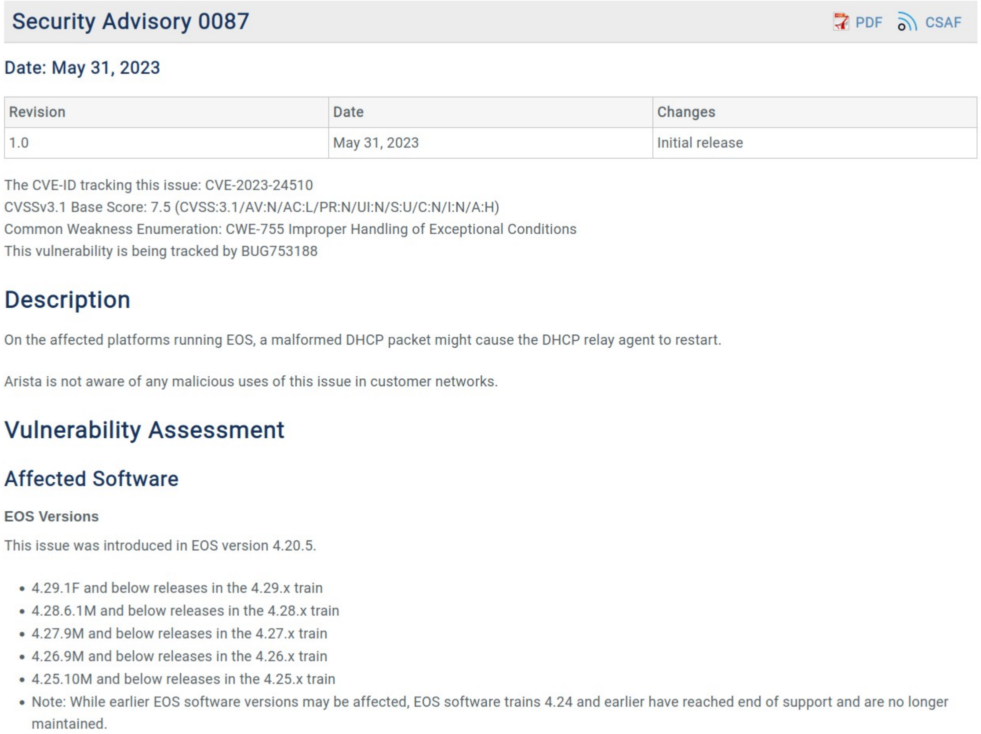
This affects the versions of SSLv3 protocol that was used in EOS version 4.12.0 through 4.12.7.1 and 4.13.0 through 4.13.6. Other versions of EOS are not affected. Additionally this vulnerability only affects systems with Arista eAPI enabled with https transport.

Exploiting this vulnerability is not easily accomplished. Man-in-the-middle attacks require large amounts of time and resources. While the likelihood is low, Arista recommends implementing only TLS to avoid flaws in SSL. The latest releases of EOS include patches for this vulnerability. A software patch (RPM extension) is available that addresses the vulnerability for releases that are affected as below:

| Releases affected | Releases not affected | Releases fixed |
|---|---|---|
| 4.12.0 through 4.12.7.1 | 4.10.x all releases | 4.12.8 or later |
| 4.13.0 through 4.13.6 | 4.11.x all releases | 4.13.7 or later |
| | Earlier releases are unaffected | 4.14.0 or later |

BugID 83779 addresses the issue.

All models of the Arista 7000 Series of fixed and modular systems are affected.



## Security Advisory 0087

PDF CSAF

**Date: May 31, 2023**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | May 31, 2023 | Initial release |

The CVE-ID tracking this issue: CVE-2023-24510
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Common Weakness Enumeration: CWE-755 Improper Handling of Exceptional Conditions
This vulnerability is being tracked by BUG753188

## Description

On the affected platforms running EOS, a malformed DHCP packet might cause the DHCP relay agent to restart.

Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

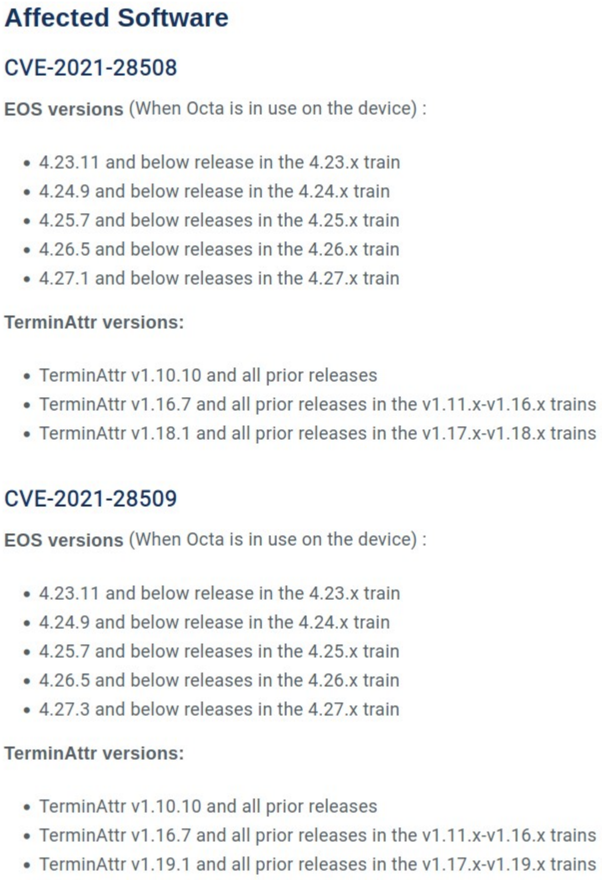
**EOS Versions**

This issue was introduced in EOS version 4.20.5.

- 4.29.1F and below releases in the 4.29.x train
- 4.28.6.1M and below releases in the 4.28.x train
- 4.27.9M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train
- 4.25.10M and below releases in the 4.25.x train
- Note: While earlier EOS software versions may be affected, EOS software trains 4.24 and earlier have reached end of support and are no longer maintained.

[1] https://www.arista.com/en/support/advisories-notices/security-advisory/1015-security-advisory-7
[2] https://www.arista.com/en/support/advisories-notices/security-advisory/17445-security-advisory-0087

# CSAF ではバージョンの表現に苦労してそう



## Affected Software

### CVE-2021-28508

**EOS versions** (When Octa is in use on the device) :

- 4.23.11 and below release in the 4.23.x train
- 4.24.9 and below release in the 4.24.x train
- 4.25.7 and below releases in the 4.25.x train
- 4.26.5 and below releases in the 4.26.x train
- 4.27.1 and below releases in the 4.27.x train

**TerminAttr versions:**

- TerminAttr v1.10.10 and all prior releases
- TerminAttr v1.16.7 and all prior releases in the v1.11.x-v1.16.x trains
- TerminAttr v1.18.1 and all prior releases in the v1.17.x-v1.18.x trains

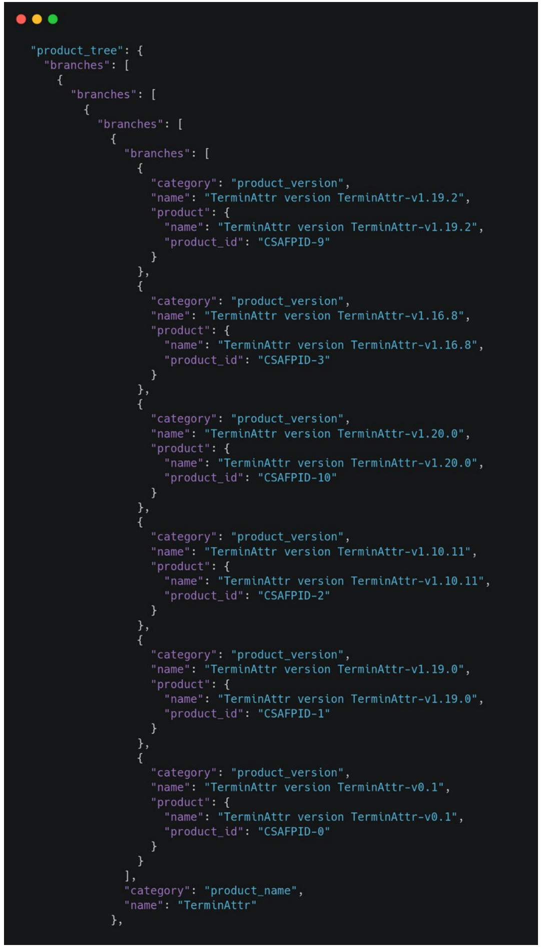
### CVE-2021-28509

**EOS versions** (When Octa is in use on the device) :

- 4.23.11 and below release in the 4.23.x train
- 4.24.9 and below release in the 4.24.x train
- 4.25.7 and below releases in the 4.25.x train
- 4.26.5 and below releases in the 4.26.x train
- 4.27.3 and below releases in the 4.27.x train

**TerminAttr versions:**

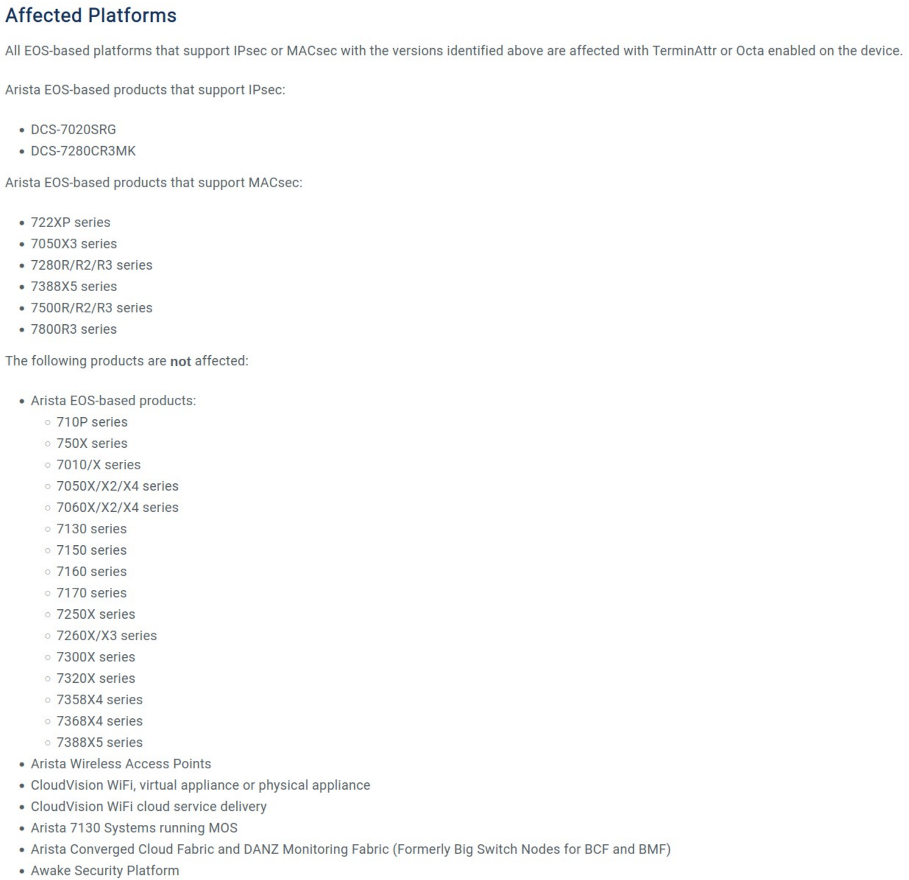
- TerminAttr v1.10.10 and all prior releases
- TerminAttr v1.16.7 and all prior releases in the v1.11.x-v1.16.x trains
- TerminAttr v1.19.1 and all prior releases in the v1.17.x-v1.19.x trains



```
"product_tree": {
  "branches": [
    {
      "branches": [
        {
          "branches": [
            {
              "branches": [
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.19.2",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.19.2",
                    "product_id": "CSAFPID-9"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.16.8",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.16.8",
                    "product_id": "CSAFPID-3"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.20.0",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.20.0",
                    "product_id": "CSAFPID-10"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.10.11",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.10.11",
                    "product_id": "CSAFPID-2"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.19.0",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.19.0",
                    "product_id": "CSAFPID-1"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v0.1",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v0.1",
                    "product_id": "CSAFPID-0"
                  }
                }
              ],
              "category": "product_name",
              "name": "TerminAttr"
            },
```

[1] https://www.arista.com/en/support/advisories-notices/security-advisory/15484-security-advisory-0077
[2] https://www.arista.com/assets/data/SecurityAdvisories/CSAF/arista_networks_security_advisory_77.json

# Affected Platforms が Web/PDF しか記述されていない



## Affected Platforms

All EOS-based platforms that support IPsec or MACsec with the versions identified above are affected with TerminAttr or Octa enabled on the device.

Arista EOS-based products that support IPsec:

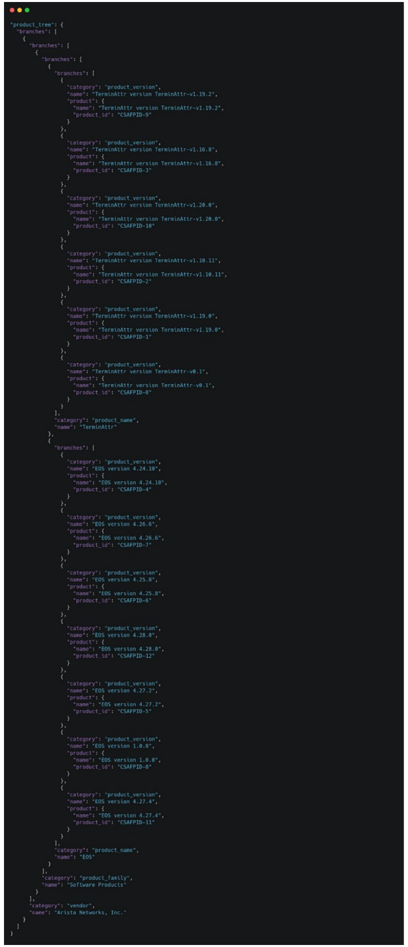
- DCS-7020SRG
- DCS-7280CR3MK

Arista EOS-based products that support MACsec:

- 722XP series
- 7050X3 series
- 7280R/R2/R3 series
- 7388X5 series
- 7500R/R2/R3 series
- 7800R3 series

The following products are **not** affected:

- Arista EOS-based products:
  - 710P series
  - 750X series
  - 7010/X series
  - 7050X/X2/X4 series
  - 7060X/X2/X4 series
  - 7130 series
  - 7150 series
  - 7160 series
  - 7170 series
  - 7250X series
  - 7260X/X3 series
  - 7300X series
  - 7320X series
  - 7358X4 series
  - 7368X4 series
  - 7388X5 series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

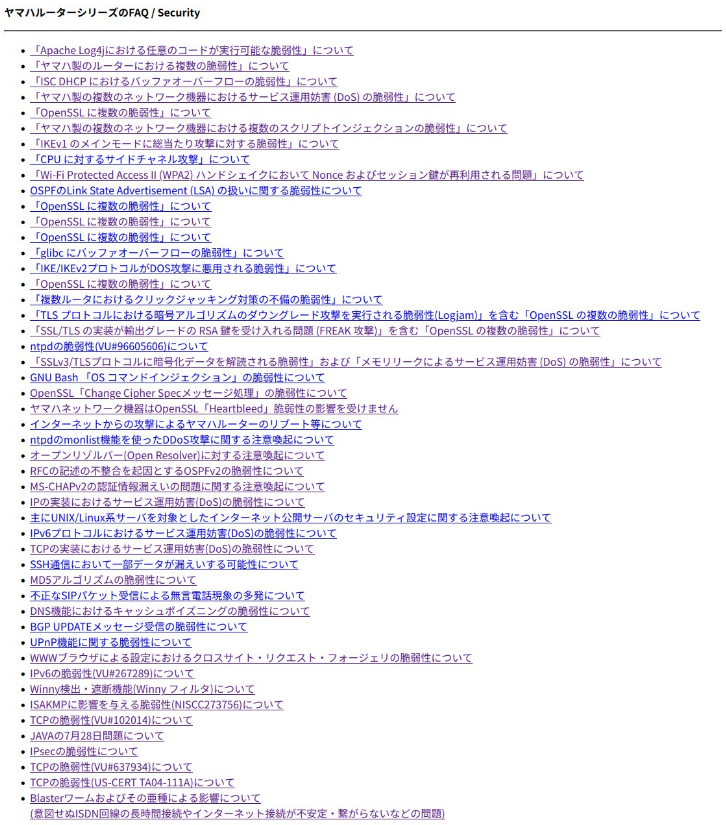


```
"product_tree": {
  "branches": [
    {
      "branches": [
        {
          "branches": [
            {
              "branches": [
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.19.2",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.19.2",
                    "product_id": "CSAFPID-9"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.16.8",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.16.8",
                    "product_id": "CSAFPID-3"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.20.0",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.20.0",
                    "product_id": "CSAFPID-10"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.10.11",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.10.11",
                    "product_id": "CSAFPID-2"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v1.19.0",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v1.19.0",
                    "product_id": "CSAFPID-1"
                  }
                },
                {
                  "category": "product_version",
                  "name": "TerminAttr version TerminAttr-v0.1",
                  "product": {
                    "name": "TerminAttr version TerminAttr-v0.1",
                    "product_id": "CSAFPID-0"
                  }
                }
              ],
              "category": "product_name",
              "name": "TerminAttr"
            },
            {
              "branches": [
                {
                  "category": "product_version",
                  "name": "EOS version 4.24.10",
                  "product": {
                    "name": "EOS version 4.24.10",
                    "product_id": "CSAFPID-4"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 4.26.6",
                  "product": {
                    "name": "EOS version 4.26.6",
                    "product_id": "CSAFPID-7"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 4.25.8",
                  "product": {
                    "name": "EOS version 4.25.8",
                    "product_id": "CSAFPID-6"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 4.28.0",
                  "product": {
                    "name": "EOS version 4.28.0",
                    "product_id": "CSAFPID-12"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 4.27.2",
                  "product": {
                    "name": "EOS version 4.27.2",
                    "product_id": "CSAFPID-5"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 1.0.0",
                  "product": {
                    "name": "EOS version 1.0.0",
                    "product_id": "CSAFPID-8"
                  }
                },
                {
                  "category": "product_version",
                  "name": "EOS version 4.27.4",
                  "product": {
                    "name": "EOS version 4.27.4",
                    "product_id": "CSAFPID-11"
                  }
                }
              ],
              "category": "product_name",
              "name": "EOS"
            }
          ],
          "category": "product_family",
          "name": "Software Products"
        }
      ],
      "category": "vendor",
      "name": "Arista Networks, Inc."
    }
  ]
}
```

[1] https://www.arista.com/en/support/advisories-notices/security-advisory/15484-security-advisory-0077
[2] https://www.arista.com/assets/data/SecurityAdvisories/CSAF/arista_networks_security_advisory_77.json

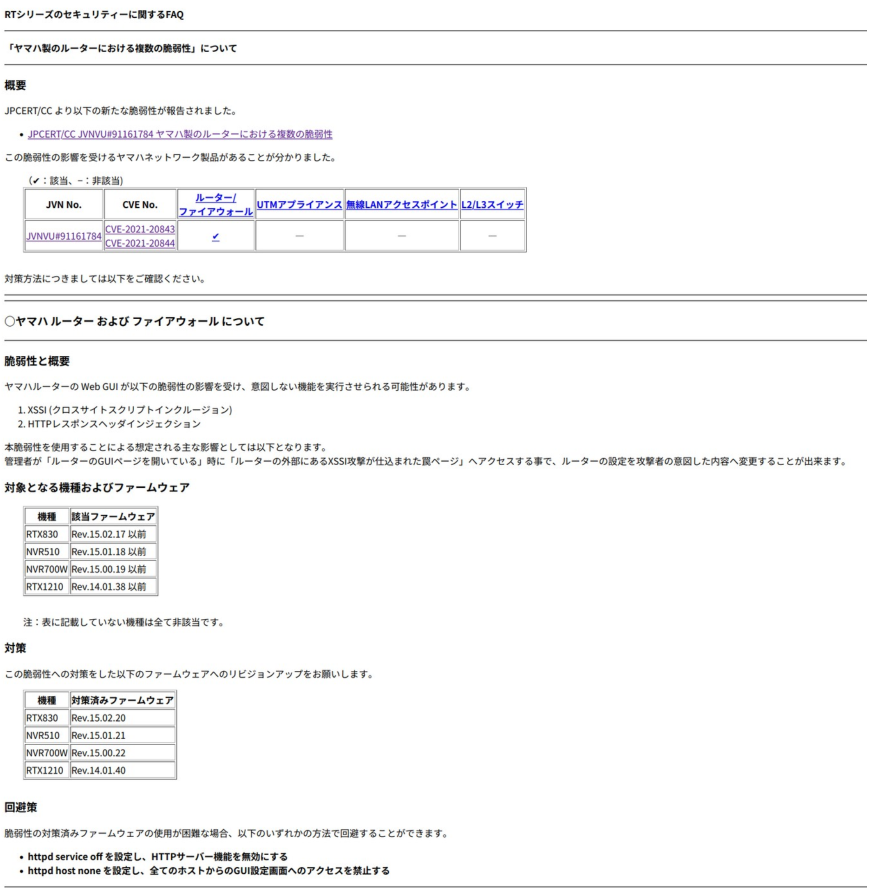
# YAMAHA

# 総アドバイザリ数 : 50 /  リスト  / Web



**ヤマハルーターシリーズのFAQ / Security**

- 「Apache Log4jにおける任意のコードが実行可能な脆弱性」について
- 「ヤマハ製のルーターにおける複数の脆弱性」について
- 「ISC DHCP におけるバッファオーバーフローの脆弱性」について
- 「ヤマハ製の複数のネットワーク機器におけるサービス運用妨害 (DoS) の脆弱性」について
- 「OpenSSL に複数の脆弱性」について
- 「ヤマハ製の複数のネットワーク機器における複数のスクリプトインジェクションの脆弱性」について
- 「IKEv1 のメインモードに総当たり攻撃に対する脆弱性」について
- 「CPU に対するサイドチャネル攻撃」について
- 「Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonce およびセッション鍵が再利用される問題」について
- OSPFのLink State Advertisement (LSA) の扱いに関する脆弱性について
- 「OpenSSL に複数の脆弱性」について
- 「OpenSSL に複数の脆弱性」について
- 「OpenSSL に複数の脆弱性」について
- 「glibc にバッファオーバーフローの脆弱性」について
- 「IKE/IKEv2プロトコルがDOS攻撃に悪用される脆弱性」について
- 「OpenSSL に複数の脆弱性」について
- 「複数ルータにおけるクリックジャッキング対策の不備の脆弱性」について
- 「TLS プロトコルにおける暗号アルゴリズムのダウングレード攻撃を実行される脆弱性(Logjam)」を含む「OpenSSL の複数の脆弱性」について
- 「SSL/TLS の実装が輸出グレードの RSA 鍵を受け入れる問題 (FREAK 攻撃)」を含む「OpenSSL の複数の脆弱性」について
- ntpdの脆弱性(VU#96605606)について
- 「SSLv3/TLSプロトコルに暗号化データを解読される脆弱性」および「メモリリークによるサービス運用妨害 (DoS) の脆弱性」について
- GNU Bash 「OS コマンドインジェクション」の脆弱性について
- OpenSSL「Change Cipher Specメッセージ処理」の脆弱性について
- ヤマハネットワーク機器はOpenSSL「Heartbleed」脆弱性の影響を受けません
- インターネットからの攻撃によるヤマハルーターのリブート等について
- ntpdのmonlist機能を使ったDDoS攻撃に関する注意喚起について
- オープンリゾルバー(Open Resolver)に対する注意喚起について
- RFCの記述の不整合を起因とするOSPFv2の脆弱性について
- MS-CHAPv2の認証情報漏えいの問題に関する注意喚起について
- IPの実装におけるサービス運用妨害(DoS)の脆弱性について
- 主にUNIX/Linux系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起について
- IPv6プロトコルにおけるサービス運用妨害(DoS)の脆弱性について
- TCPの実装におけるサービス運用妨害(DoS)の脆弱性について
- SSH通信において一部データが漏えいする可能性について
- MD5アルゴリズムの脆弱性について
- 不正なSIPパケット受信による無言電話現象の多発について
- DNS機能におけるキャッシュポイズニングの脆弱性について
- BGP UPDATEメッセージ受信の脆弱性について
- UPnP機能に関する脆弱性について
- WWWブラウザによる設定におけるクロスサイト・リクエスト・フォージェリの脆弱性について
- IPv6の脆弱性(VU#267289)について
- Winny検出・遮断機能(Winny フィルタ)について
- ISAKMPに影響を与える脆弱性(NISCC273756)について
- TCPの脆弱性(VU#102014)について
- JAVAの7月28日問題について
- IPsecの脆弱性について
- TCPの脆弱性(VU#637934)について
- TCPの脆弱性(US-CERT TA04-111A)について
- Blasterワームおよびその亜種による影響について
  (意図せぬISDN回線の長時間接続やインターネット接続が不安定・繋がらないなどの問題)



**RTシリーズのセキュリティーに関するFAQ**

**「ヤマハ製のルーターにおける複数の脆弱性」について**

**概要**

JPCERT/CC より以下の新たな脆弱性が報告されました。

- JPCERT/CC JVNVU#91161784 ヤマハ製のルーターにおける複数の脆弱性

この脆弱性の影響を受けるヤマハネットワーク製品があることが分かりました。

(✔：該当、－：非該当)

| JVN No. | CVE No. | ルーター/<br>ファイアウォール | UTMアプライアンス | 無線LANアクセスポイント | L2/L3スイッチ |
|---|---|---|---|---|---|
| JVNVU#91161784 | CVE-2021-20843<br>CVE-2021-20844 | ✔ | － | － | － |

対策方法につきましては以下をご確認ください。

**○ヤマハ ルーター および ファイアウォール について**

**脆弱性と概要**

ヤマハルーターの Web GUI が以下の脆弱性の影響を受け、意図しない機能を実行させられる可能性があります。

1. XSSI (クロスサイトスクリプトインクルージョン)
2. HTTPレスポンスヘッダインジェクション

本脆弱性を使用することによる想定される主な影響としては以下となります。
管理者が「ルーターのGUIページを開いている」時に「ルーターの外部にあるXSSI攻撃が仕込まれた罠ページ」へアクセスする事で、ルーターの設定を攻撃者の意図した内容へ変更することが出来ます。

**対象となる機種およびファームウェア**

| 機種 | 該当ファームウェア |
|---|---|
| RTX830 | Rev.15.02.17 以前 |
| NVR510 | Rev.15.01.18 以前 |
| NVR700W | Rev.15.00.19 以前 |
| RTX1210 | Rev.14.01.38 以前 |

注：表に記載していない機種は全て非該当です。

**対策**

この脆弱性への対策をした以下のファームウェアへのリビジョンアップをお願いします。

| 機種 | 対策済みファームウェア |
|---|---|
| RTX830 | Rev.15.02.20 |
| NVR510 | Rev.15.01.21 |
| NVR700W | Rev.15.00.22 |
| RTX1210 | Rev.14.01.40 |

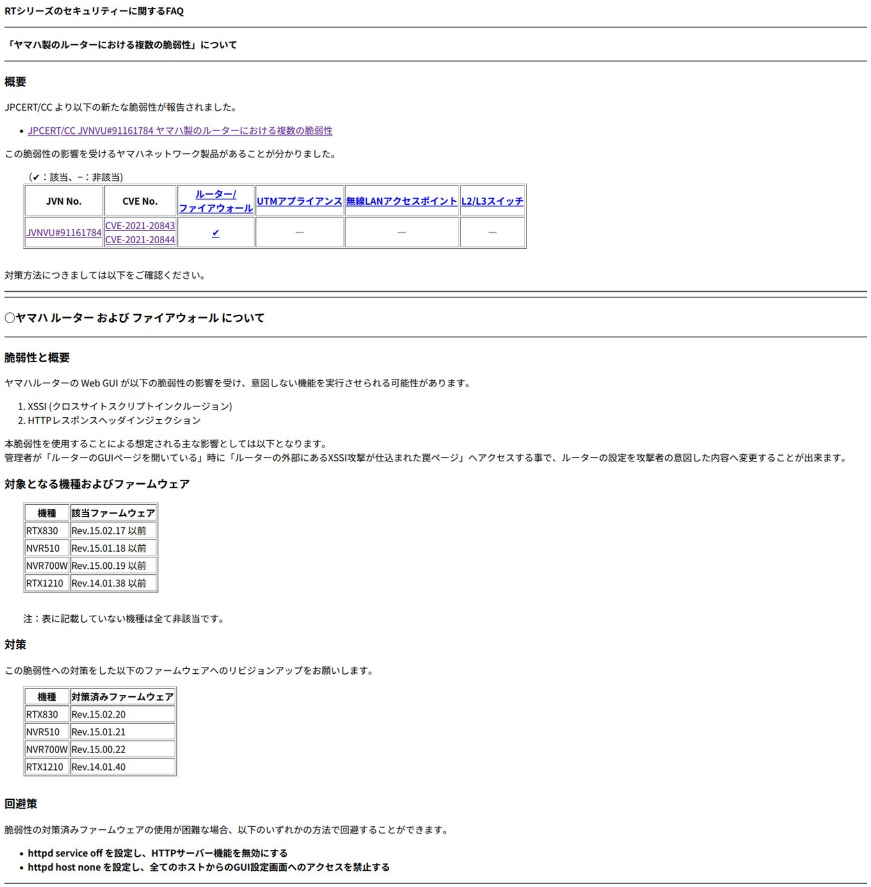
**回避策**

脆弱性の対策済みファームウェアの使用が困難な場合、以下のいずれかの方法で回避することができます。

- **httpd service off を設定し、HTTPサーバー機能を無効にする**
- **httpd host none を設定し、全てのホストからのGUI設定画面へのアクセスを禁止する**

http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/index.html

# affected 部分などフォーマットが異なる



**RTシリーズのセキュリティーに関するFAQ**

**「ヤマハ製のルーターにおける複数の脆弱性」について**

### 概要

JPCERT/CC より以下の新たな脆弱性が報告されました。

- JPCERT/CC JVNVU#91161784 ヤマハ製のルーターにおける複数の脆弱性

この脆弱性の影響を受けるヤマハネットワーク製品があることが分かりました。

(✔：該当、－：非該当)

| JVN No. | CVE No. | ルーター/<br>ファイアウォール | UTMアプライアンス | 無線LANアクセスポイント | L2/L3スイッチ |
|---|---|---|---|---|---|
| JVNVU#91161784 | CVE-2021-20843<br>CVE-2021-20844 | ✔ | — | — | — |

対策方法につきましては以下をご確認ください。

### ○ヤマハ ルーター および ファイアウォール について

### 脆弱性と概要

ヤマハルーターの Web GUI が以下の脆弱性の影響を受け、意図しない機能を実行させられる可能性があります。

1. XSSI (クロスサイトスクリプトインクルージョン)
2. HTTPレスポンスヘッダインジェクション

本脆弱性を使用することによる想定される主な影響としては以下となります。
管理者が「ルーターのGUIページを開いている」時に「ルーターの外部にあるXSSI攻撃が仕込まれた罠ページ」へアクセスする事で、ルーターの設定を攻撃者の意図した内容へ変更することが出来ます。

### 対象となる機種およびファームウェア

| 機種 | 該当ファームウェア |
|---|---|
| RTX830 | Rev.15.02.17 以前 |
| NVR510 | Rev.15.01.18 以前 |
| NVR700W | Rev.15.00.19 以前 |
| RTX1210 | Rev.14.01.38 以前 |

注：表に記載していない機種は全て非該当です。

### 対策

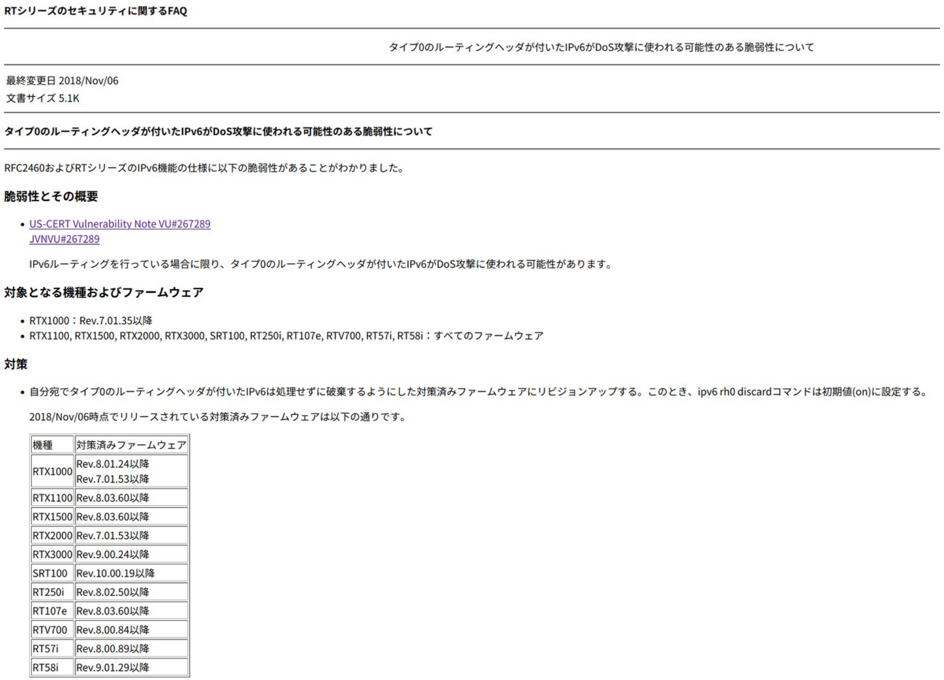
この脆弱性への対策をした以下のファームウェアへのリビジョンアップをお願いします。

| 機種 | 対策済みファームウェア |
|---|---|
| RTX830 | Rev.15.02.20 |
| NVR510 | Rev.15.01.21 |
| NVR700W | Rev.15.00.22 |
| RTX1210 | Rev.14.01.40 |

### 回避策

脆弱性の対策済みファームウェアの使用が困難な場合、以下のいずれかの方法で回避することができます。

- **httpd service off を設定し、HTTPサーバー機能を無効にする**
- **httpd host none を設定し、全てのホストからのGUI設定画面へのアクセスを禁止する**



**RTシリーズのセキュリティに関するFAQ**

タイプ0のルーティングヘッダが付いたIPv6がDoS攻撃に使われる可能性のある脆弱性について

最終変更日 2018/Nov/06
文書サイズ 5.1K

**タイプ0のルーティングヘッダが付いたIPv6がDoS攻撃に使われる可能性のある脆弱性について**

RFC2460およびRTシリーズのIPv6機能の仕様に以下の脆弱性があることがわかりました。

### 脆弱性とその概要

- US-CERT Vulnerability Note VU#267289
  JVNVU#267289

  IPv6ルーティングを行っている場合に限り、タイプ0のルーティングヘッダが付いたIPv6がDoS攻撃に使われる可能性があります。

### 対象となる機種およびファームウェア

- RTX1000：Rev.7.01.35以降
- RTX1100, RTX1500, RTX2000, RTX3000, SRT100, RT250i, RT107e, RTV700, RT57i, RT58i：すべてのファームウェア

### 対策

- 自分宛でタイプ0のルーティングヘッダが付いたIPv6は処理せずに破棄するようにした対策済みファームウェアにリビジョンアップする。このとき、ipv6 rh0 discardコマンドは初期値(on)に設定する。

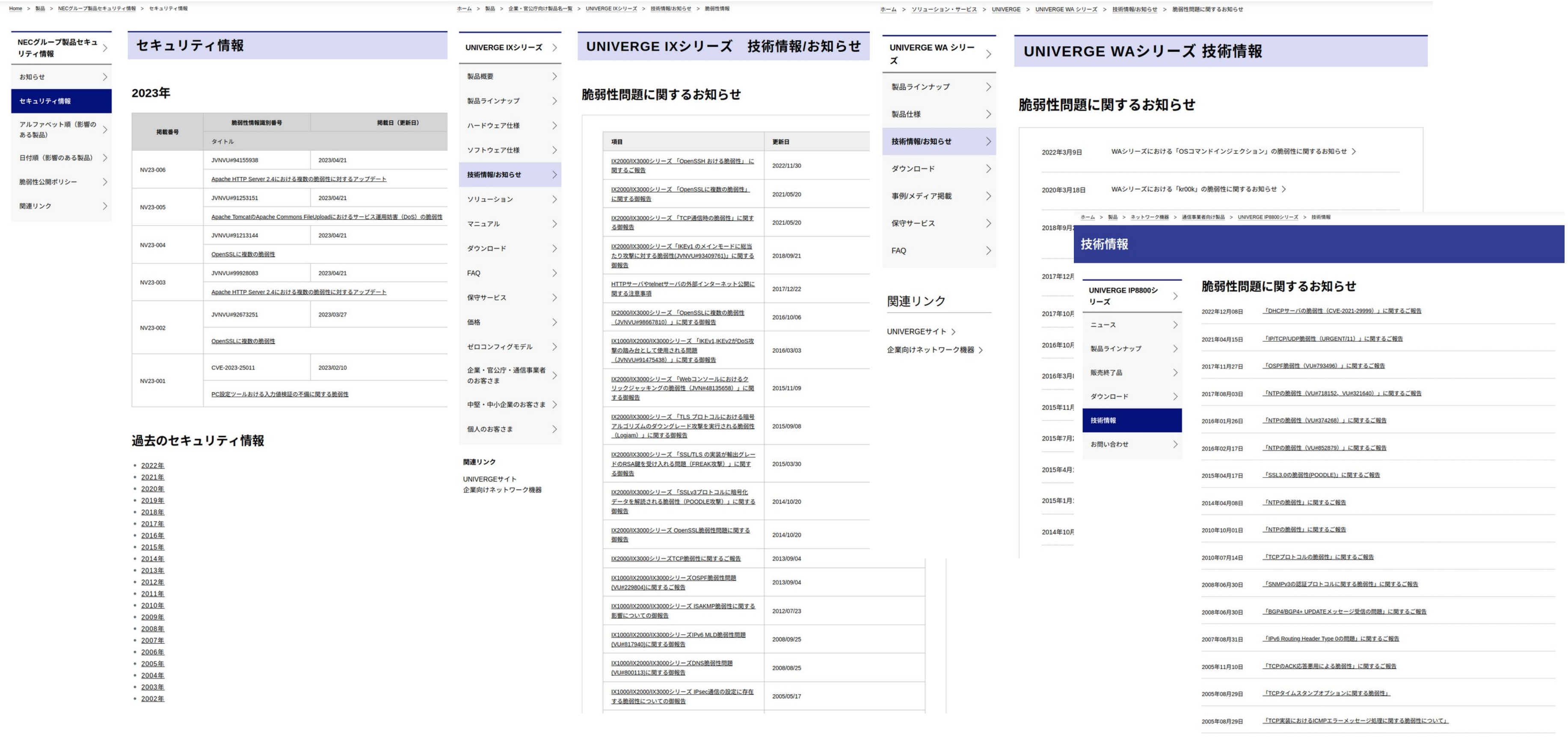
  2018/Nov/06時点でリリースされている対策済みファームウェアは以下の通りです。

| 機種 | 対策済みファームウェア |
|---|---|
| RTX1000 | Rev.8.01.24以降<br>Rev.7.01.53以降 |
| RTX1100 | Rev.8.03.60以降 |
| RTX1500 | Rev.8.03.60以降 |
| RTX2000 | Rev.7.01.53以降 |
| RTX3000 | Rev.9.00.24以降 |
| SRT100 | Rev.10.00.19以降 |
| RT250i | Rev.8.02.50以降 |
| RT107e | Rev.8.03.60以降 |
| RTV700 | Rev.8.00.84以降 |
| RT57i | Rev.8.00.89以降 |
| RT58i | Rev.9.01.29以降 |

[1] http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html
[2] http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU267289.html

# NEC

# 総アドバイザリ数：? / リスト / Web



Home > 製品 > NECグループ製品セキュリティ情報 > セキュリティ情報

## セキュリティ情報

### 2023年

| 掲載番号 | 脆弱性情報識別番号 | 掲載日（更新日） |
|---|---|---|
| | タイトル | |
| NV23-006 | JVNVU#94155938 | 2023/04/21 |
| | Apache HTTP Server 2.4における複数の脆弱性に対するアップデート | |
| NV23-005 | JVNVU#91253151 | 2023/04/21 |
| | Apache TomcatのApache Commons FileUploadにおけるサービス運用妨害（DoS）の脆弱性 | |
| NV23-004 | JVNVU#91213144 | 2023/04/21 |
| | OpenSSLに複数の脆弱性 | |
| NV23-003 | JVNVU#99928083 | 2023/04/21 |
| | Apache HTTP Server 2.4における複数の脆弱性に対するアップデート | |
| NV23-002 | JVNVU#92673251 | 2023/03/27 |
| | OpenSSLに複数の脆弱性 | |
| NV23-001 | CVE-2023-25011 | 2023/02/10 |
| | PC設定ツールおける入力値検証の不備に関する脆弱性 | |

### 過去のセキュリティ情報

- 2022年
- 2021年
- 2020年
- 2019年
- 2018年
- 2017年
- 2016年
- 2015年
- 2014年
- 2013年
- 2012年
- 2011年
- 2010年
- 2009年
- 2008年
- 2007年
- 2006年
- 2005年
- 2004年
- 2003年
- 2002年

ホーム > 製品 > 企業・官公庁向け製品名一覧 > UNIVERGE IXシリーズ > 技術情報/お知らせ > 脆弱性情報

## UNIVERGE IXシリーズ　技術情報/お知らせ

### 脆弱性問題に関するお知らせ

| 項目 | 更新日 |
|---|---|
| IX2000/IX3000シリーズ 「OpenSSH おける脆弱性」 に関するご報告 | 2022/11/30 |
| IX2000/IX3000シリーズ 「OpenSSLに複数の脆弱性」 に関する御報告 | 2021/05/20 |
| IX2000/IX3000シリーズ 「TCP通信時の脆弱性」に関する御報告 | 2021/05/20 |
| IX2000/IX3000シリーズ「IKEv1 のメインモードに総当たり攻撃に対する脆弱性(JVNVU#93409761)」に関する御報告 | 2018/09/21 |
| HTTPサーバやtelnetサーバの外部インターネット公開に関する注意事項 | 2017/12/22 |
| IX2000/IX3000シリーズ 「OpenSSLに複数の脆弱性（JVNVU#98667810）」に関する御報告 | 2016/10/06 |
| IX1000/IX2000/IX3000シリーズ 「IKEv1,IKEv2がDoS攻撃の踏み台として使用される問題（JVNVU#91475438）」に関する御報告 | 2016/03/03 |
| IX2000/IX3000シリーズ 「Webコンソールにおけるクリックジャッキングの脆弱性（JVN#48135658）」に関する御報告 | 2015/11/09 |
| IX2000/IX3000シリーズ 「TLS プロトコルにおける暗号アルゴリズムのダウングレード攻撃を実行される脆弱性（Logjam）」に関する御報告 | 2015/09/08 |
| IX2000/IX3000シリーズ 「SSL/TLS の実装が輸出グレードのRSA鍵を受け入れる問題（FREAK攻撃）」に関する御報告 | 2015/03/30 |
| IX2000/IX3000シリーズ 「SSLv3プロトコルに暗号化データを解読される脆弱性（POODLE攻撃）」に関する御報告 | 2014/10/20 |
| IX2000/IX3000シリーズ OpenSSL脆弱性問題に関する御報告 | 2014/10/20 |
| IX2000/IX3000シリーズTCP脆弱性に関するご報告 | 2013/09/04 |
| IX1000/IX2000/IX3000シリーズOSPF脆弱性問題(VU#229804)に関するご報告 | 2013/09/04 |
| IX1000/IX2000/IX3000シリーズ ISAKMP脆弱性に関する影響についての御報告 | 2012/07/23 |
| IX1000/IX2000/IX3000シリーズIPv6 MLD脆弱性問題(VU#817940)に関する御報告 | 2008/09/25 |
| IX1000/IX2000/IX3000シリーズDNS脆弱性問題(VU#800113)に関する御報告 | 2008/08/25 |
| IX1000/IX2000/IX3000シリーズ IPsec通信の設定に存在する脆弱性についての御報告 | 2005/05/17 |

ホーム > ソリューション・サービス > UNIVERGE > UNIVERGE WA シリーズ > 技術情報/お知らせ > 脆弱性問題に関するお知らせ

## UNIVERGE WAシリーズ 技術情報

### 脆弱性問題に関するお知らせ

| | |
|---|---|
| 2022年3月9日 | WAシリーズにおける「OSコマンドインジェクション」の脆弱性に関するお知らせ |
| 2020年3月18日 | WAシリーズにおける「kr00k」の脆弱性に関するお知らせ |
| 2018年9月 | |
| 2017年12月 | |
| 2017年10月 | |
| 2016年10月 | |
| 2016年3月 | |
| 2015年11月 | |
| 2015年7月 | |
| 2015年4月 | |
| 2015年1月 | |
| 2014年10月 | |

ホーム > 製品 > ネットワーク機器 > 通信事業者向け製品 > UNIVERGE IP8800シリーズ > 技術情報

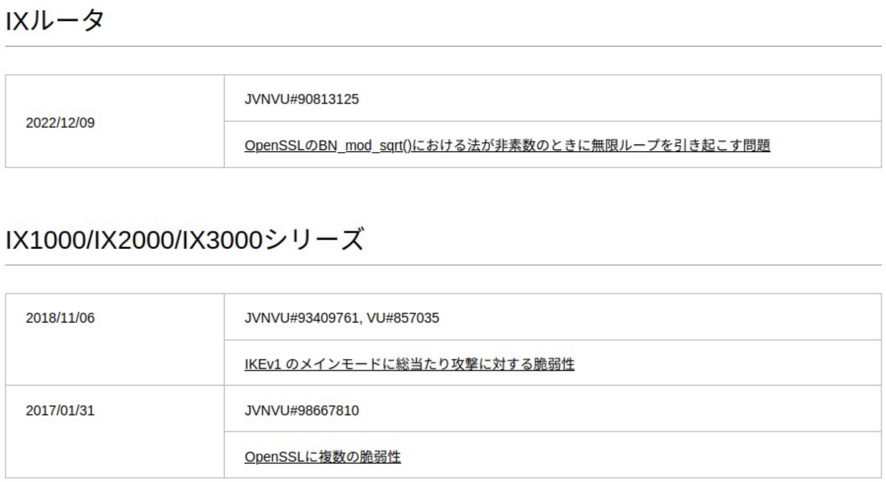
## 技術情報

### 脆弱性問題に関するお知らせ

| | |
|---|---|
| 2022年12月08日 | 「DHCPサーバの脆弱性（CVE-2021-29999）」に関するご報告 |
| 2021年04月15日 | 「IP/TCP/UDP脆弱性（URGENT/11）」に関するご報告 |
| 2017年11月27日 | 「OSPF脆弱性（VU#793496）」に関するご報告 |
| 2017年08月03日 | 「NTPの脆弱性（VU#718152、VU#321640）」に関するご報告 |
| 2016年01月26日 | 「NTPの脆弱性（VU#374268）」に関するご報告 |
| 2016年02月17日 | 「NTPの脆弱性（VU#852879）」に関するご報告 |
| 2015年04月17日 | 「SSL3.0の脆弱性(POODLE)」に関するご報告 |
| 2014年04月08日 | 「NTPの脆弱性」に関するご報告 |
| 2010年10月01日 | 「NTPの脆弱性」に関するご報告 |
| 2010年07月14日 | 「TCPプロトコルの脆弱性」に関するご報告 |
| 2008年06月30日 | 「SNMPv3の認証プロトコルに関する脆弱性」に関するご報告 |
| 2008年06月30日 | 「BGP4/BGP4+ UPDATEメッセージ受信の問題」に関するご報告 |
| 2007年08月31日 | 「IPv6 Routing Header Type 0の問題」に関するご報告 |
| 2005年11月10日 | 「TCPのACK応答悪用による脆弱性」に関するご報告 |
| 2005年08月29日 | 「TCPタイムスタンプオプションに関する脆弱性」 |
| 2005年08月29日 | 「TCP実装におけるICMPエラーメッセージ処理に関する脆弱性について」 |

[1] https://jpn.nec.com/security-info/sec.html [2] https://jpn.nec.com/univerge/ix/Support/Security-Info/index.html
[3] https://jpn.nec.com/univerge/wa/info/zeijaku.html [4] https://jpn.nec.com/ip88n/tech.html

IXルータに関するアドバイザリは2箇所で掲載されている（アドバイザリリストを分割する意味がない

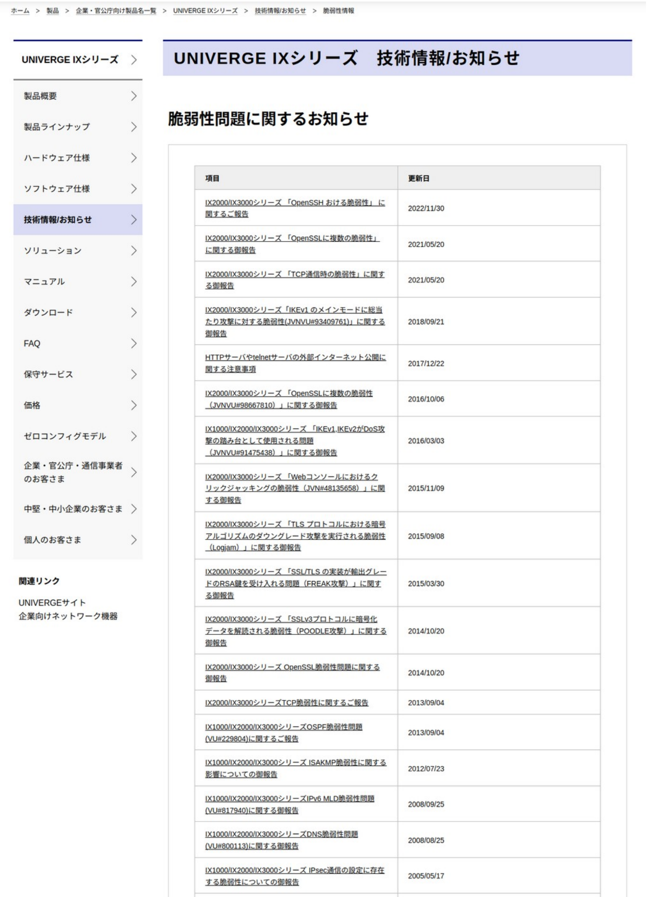


## IXルータ

| | |
|---|---|
| 2022/12/09 | JVNVU#90813125 |
| | OpenSSLのBN_mod_sqrt()における法が非素数のときに無限ループを引き起こす問題 |

## IX1000/IX2000/IX3000シリーズ

| | |
|---|---|
| 2018/11/06 | JVNVU#93409761, VU#857035 |
| | IKEv1 のメインモードに総当たり攻撃に対する脆弱性 |
| 2017/01/31 | JVNVU#98667810 |
| | OpenSSLに複数の脆弱性 |



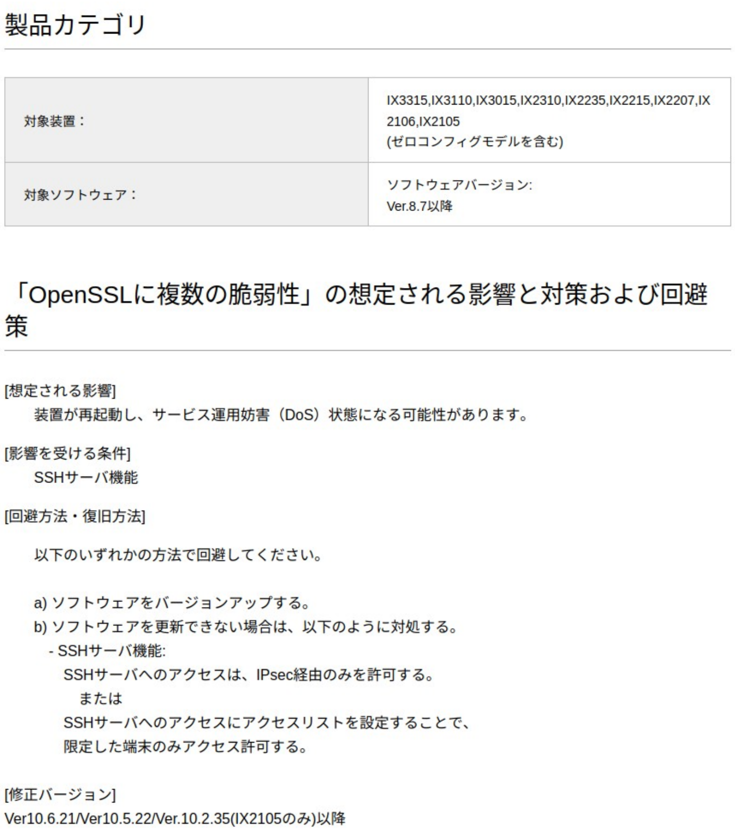
### UNIVERGE IXシリーズ　技術情報/お知らせ

#### 脆弱性問題に関するお知らせ

| 項目 | 更新日 |
|---|---|
| IX2000/IX3000シリーズ 「OpenSSH おける脆弱性」 に関するご報告 | 2022/11/30 |
| IX2000/IX3000シリーズ 「OpenSSLに複数の脆弱性」 に関する御報告 | 2021/05/20 |
| IX2000/IX3000シリーズ 「TCP通信時の脆弱性」に関する御報告 | 2021/05/20 |
| IX2000/IX3000シリーズ「IKEv1 のメインモードに総当たり攻撃に対する脆弱性(JVNVU#93409761)」に関する御報告 | 2018/09/21 |
| HTTPサーバやtelnetサーバの外部インターネット公開に関する注意事項 | 2017/12/22 |
| IX2000/IX3000シリーズ 「OpenSSLに複数の脆弱性（JVNVU#98667810）」に関する御報告 | 2016/10/06 |
| IX1000/IX2000/IX3000シリーズ 「IKEv1,IKEv2がDoS攻撃の踏み台として使用される問題（JVNVU#91475438）」に関する御報告 | 2016/03/03 |
| IX2000/IX3000シリーズ 「Webコンソールにおけるクリックジャッキングの脆弱性（JVN#48135658）」に関する御報告 | 2015/11/09 |
| IX2000/IX3000シリーズ 「TLS プロトコルにおける暗号アルゴリズムのダウングレード攻撃を実行される脆弱性（Logjam）」に関する御報告 | 2015/09/08 |
| IX2000/IX3000シリーズ 「SSL/TLS の実装が輸出グレードのRSA鍵を受け入れる問題（FREAK攻撃）」に関する御報告 | 2015/03/30 |
| IX2000/IX3000シリーズ 「SSLv3プロトコルに暗号化データを解読される脆弱性（POODLE攻撃）」に関する御報告 | 2014/10/20 |
| IX2000/IX3000シリーズ OpenSSL脆弱性問題に関する御報告 | 2014/10/20 |
| IX2000/IX3000シリーズTCP脆弱性に関するご報告 | 2013/09/04 |
| IX1000/IX2000/IX3000シリーズOSPF脆弱性問題(VU#229804)に関するご報告 | 2013/09/04 |
| IX1000/IX2000/IX3000シリーズ ISAKMP脆弱性に関する影響についての御報告 | 2012/07/23 |
| IX1000/IX2000/IX3000シリーズIPv6 MLD脆弱性問題(VU#817940)に関する御報告 | 2008/09/25 |
| IX1000/IX2000/IX3000シリーズDNS脆弱性問題(VU#800113)に関する御報告 | 2008/08/25 |
| IX1000/IX2000/IX3000シリーズ IPsec通信の設定に存在する脆弱性についての御報告 | 2005/05/17 |

[1] https://jpn.nec.com/security-info/sec.html [2] https://jpn.nec.com/univerge/ix/Support/Security-Info/index.html

# あるアドバイザリリストの中で、アドバイザリのフォーマットが統一されていない



## 製品カテゴリ

| | |
|---|---|
| 対象装置： | IX3315,IX3110,IX3015,IX2310,IX2235,IX2215,IX2207,IX2106,IX2105<br>(ゼロコンフィグモデルを含む) |
| 対象ソフトウェア： | ソフトウェアバージョン:<br>Ver.8.7以降 |

## 「OpenSSLに複数の脆弱性」の想定される影響と対策および回避策

[想定される影響]
　装置が再起動し、サービス運用妨害（DoS）状態になる可能性があります。

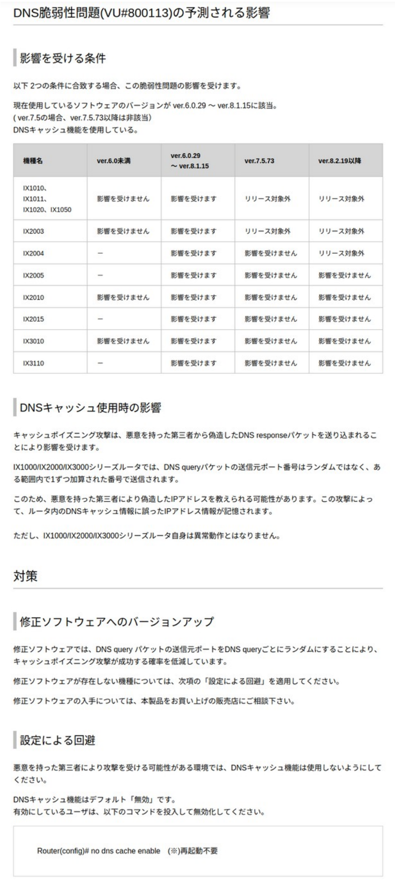
[影響を受ける条件]
　SSHサーバ機能

[回避方法・復旧方法]

　以下のいずれかの方法で回避してください。

　a) ソフトウェアをバージョンアップする。
　b) ソフトウェアを更新できない場合は、以下のように対処する。
　　- SSHサーバ機能:
　　　SSHサーバへのアクセスは、IPsec経由のみを許可する。
　　　　または
　　　SSHサーバへのアクセスにアクセスリストを設定することで、
　　　限定した端末のみアクセス許可する。

[修正バージョン]
Ver10.6.21/Ver10.5.22/Ver.10.2.35(IX2105のみ)以降



## DNS脆弱性問題(VU#800113)の予測される影響

### 影響を受ける条件

以下 2つの条件に合致する場合、この脆弱性問題の影響を受けます。

現在使用しているソフトウェアのバージョンが ver.6.0.29 ～ ver.8.1.15に該当。
( ver.7.5の場合、ver.7.5.73以降は非該当）
DNSキャッシュ機能を使用している。

| 機種名 | ver.6.0未満 | ver.6.0.29<br>～ ver.8.1.15 | ver.7.5.73 | ver.8.2.19以降 |
|---|---|---|---|---|
| IX1010、<br>IX1011、<br>IX1020、IX1050 | 影響を受けません | 影響を受けます | リリース対象外 | リリース対象外 |
| IX2003 | 影響を受けません | 影響を受けます | リリース対象外 | リリース対象外 |
| IX2004 | － | 影響を受けます | 影響を受けません | リリース対象外 |
| IX2005 | － | 影響を受けます | 影響を受けません | 影響を受けません |
| IX2010 | 影響を受けません | 影響を受けます | 影響を受けません | 影響を受けません |
| IX2015 | － | 影響を受けます | 影響を受けません | 影響を受けません |
| IX3010 | 影響を受けません | 影響を受けます | 影響を受けません | 影響を受けません |
| IX3110 | － | 影響を受けます | 影響を受けません | 影響を受けません |

### DNSキャッシュ使用時の影響

キャッシュポイズニング攻撃は、悪意を持った第三者から偽造したDNS responseパケットを送り込まれることにより影響を受けます。

IX1000/IX2000/IX3000シリーズルータでは、DNS queryパケットの送信元ポート番号はランダムではなく、ある範囲内で1ずつ加算された番号で送信されます。

このため、悪意を持った第三者により偽造したIPアドレスを教えられる可能性があります。この攻撃によって、ルータ内のDNSキャッシュ情報に誤ったIPアドレス情報が記憶されます。

ただし、IX1000/IX2000/IX3000シリーズルータ自身は異常動作とはなりません。

## 対策

### 修正ソフトウェアへのバージョンアップ

修正ソフトウェアでは、DNS query パケットの送信元ポートをDNS queryごとにランダムにすることにより、キャッシュポイズニング攻撃が成功する確率を低減しています。

修正ソフトウェアが存在しない機種については、次項の「設定による回避」を適用してください。

修正ソフトウェアの入手については、本製品をお買い上げの販売店にご相談下さい。

### 設定による回避

悪意を持った第三者により攻撃を受ける可能性がある環境では、DNSキャッシュ機能は使用しないようにしてください。

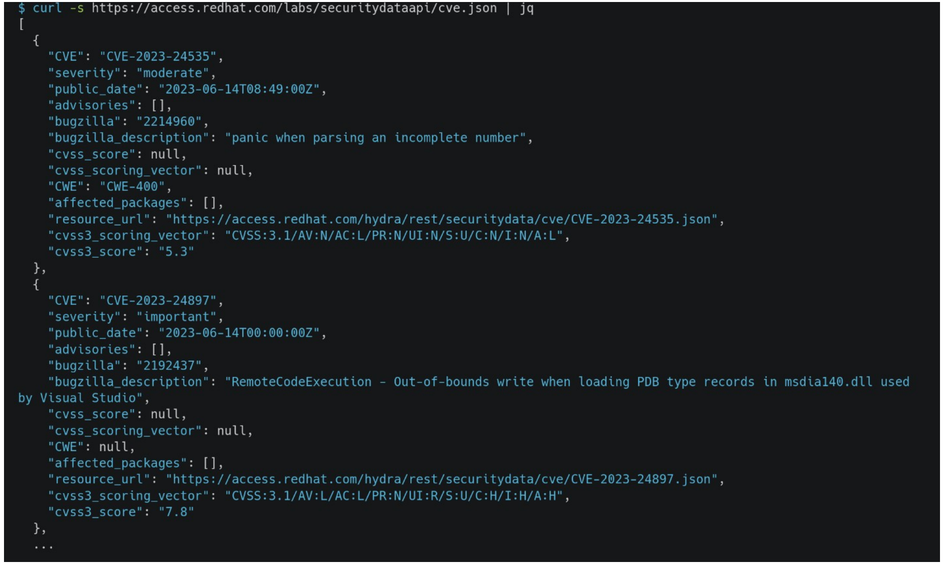
DNSキャッシュ機能はデフォルト「無効」です。
有効にしているユーザは、以下のコマンドを投入して無効化してください。

```
Router(config)# no dns cache enable   (※)再起動不要
```

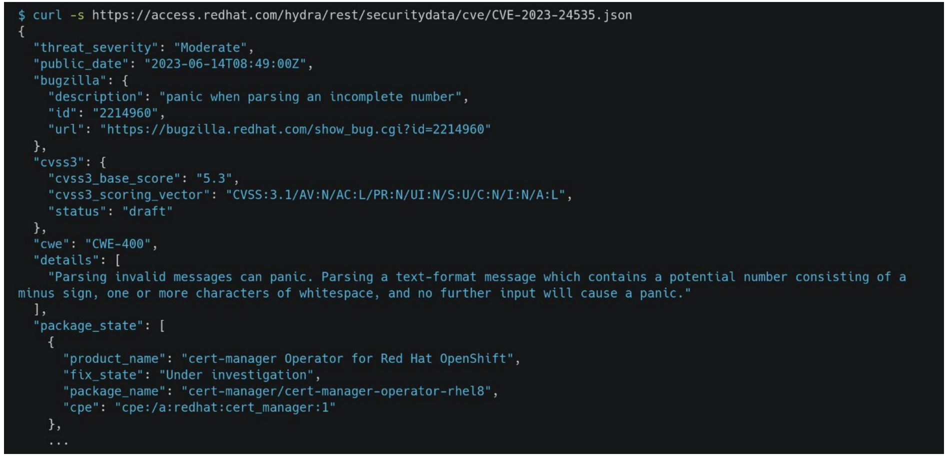
[1] https://jpn.nec.com/univerge/ix/Support/Security-Info/JVNDB-2016-008892.html
[2] https://jpn.nec.com/univerge/ix/Support/CERT/vu800113.html

# Appendix B:
# SW 界隈の脆弱性アドバイザリ公開体制

# API

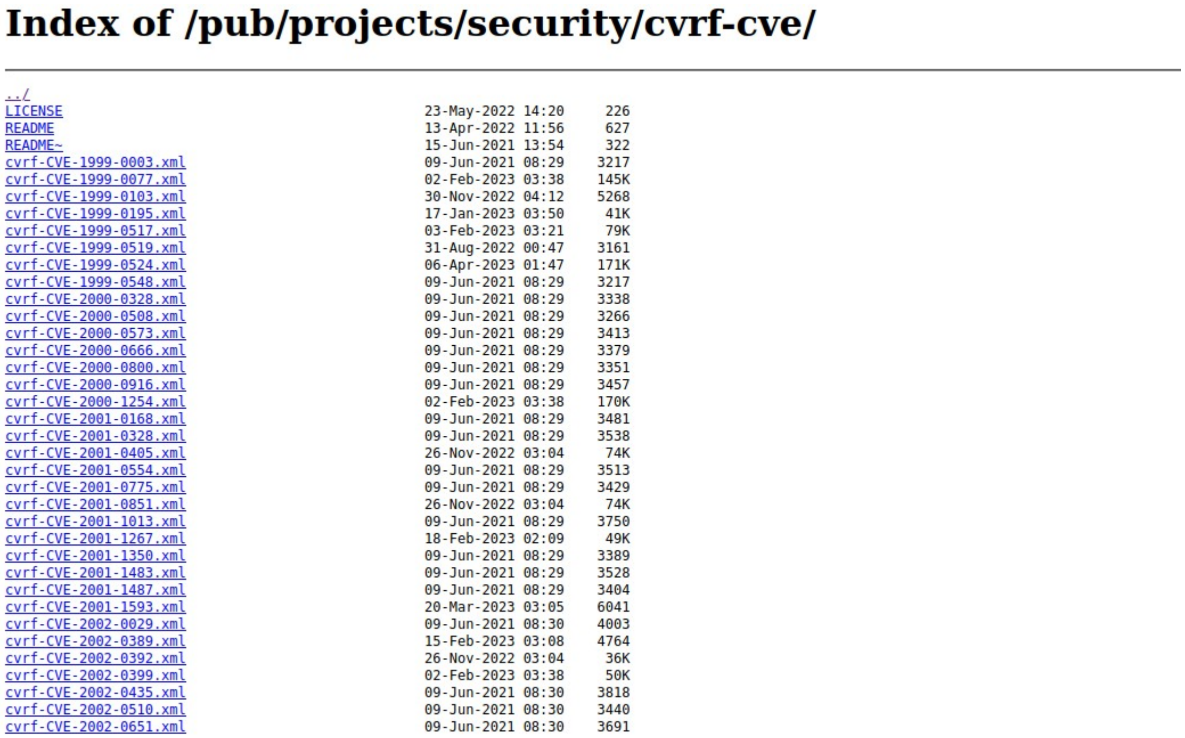


```
$ curl -s https://access.redhat.com/labs/securitydataapi/cve.json | jq
[
  {
    "CVE": "CVE-2023-24535",
    "severity": "moderate",
    "public_date": "2023-06-14T08:49:00Z",
    "advisories": [],
    "bugzilla": "2214960",
    "bugzilla_description": "panic when parsing an incomplete number",
    "cvss_score": null,
    "cvss_scoring_vector": null,
    "CWE": "CWE-400",
    "affected_packages": [],
    "resource_url": "https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2023-24535.json",
    "cvss3_scoring_vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L",
    "cvss3_score": "5.3"
  },
  {
    "CVE": "CVE-2023-24897",
    "severity": "important",
    "public_date": "2023-06-14T00:00:00Z",
    "advisories": [],
    "bugzilla": "2192437",
    "bugzilla_description": "RemoteCodeExecution - Out-of-bounds write when loading PDB type records in msdia140.dll used
by Visual Studio",
    "cvss_score": null,
    "cvss_scoring_vector": null,
    "CWE": null,
    "affected_packages": [],
    "resource_url": "https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2023-24897.json",
    "cvss3_scoring_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",
    "cvss3_score": "7.8"
  },
  ...
```



```
$ curl -s https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2023-24535.json
{
  "threat_severity": "Moderate",
  "public_date": "2023-06-14T08:49:00Z",
  "bugzilla": {
    "description": "panic when parsing an incomplete number",
    "id": "2214960",
    "url": "https://bugzilla.redhat.com/show_bug.cgi?id=2214960"
  },
  "cvss3": {
    "cvss3_base_score": "5.3",
    "cvss3_scoring_vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L",
    "status": "draft"
  },
  "cwe": "CWE-400",
  "details": [
    "Parsing invalid messages can panic. Parsing a text-format message which contains a potential number consisting of a
minus sign, one or more characters of whitespace, and no further input will cause a panic."
  ],
  "package_state": [
    {
      "product_name": "cert-manager Operator for Red Hat OpenShift",
      "fix_state": "Under investigation",
      "package_name": "cert-manager/cert-manager-operator-rhel8",
      "cpe": "cpe:/a:redhat:cert_manager:1"
    },
    ...
```

# Index of

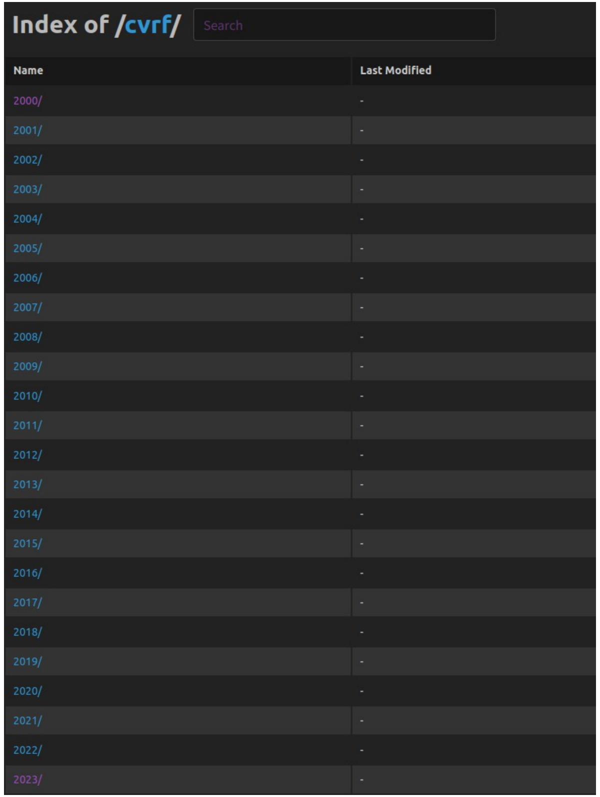


## Index of /pub/projects/security/cvrf-cve/

```
../
LICENSE                                            23-May-2022 14:20     226
README                                             13-Apr-2022 11:56     627
README~                                            15-Jun-2021 13:54     322
cvrf-CVE-1999-0003.xml                             09-Jun-2021 08:29    3217
cvrf-CVE-1999-0077.xml                             02-Feb-2023 03:38    145K
cvrf-CVE-1999-0103.xml                             30-Nov-2022 04:12    5268
cvrf-CVE-1999-0195.xml                             17-Jan-2023 03:50     41K
cvrf-CVE-1999-0517.xml                             03-Feb-2023 03:21     79K
cvrf-CVE-1999-0519.xml                             31-Aug-2022 00:47    3161
cvrf-CVE-1999-0524.xml                             06-Apr-2023 01:47    171K
cvrf-CVE-1999-0548.xml                             09-Jun-2021 08:29    3217
cvrf-CVE-2000-0328.xml                             09-Jun-2021 08:29    3338
cvrf-CVE-2000-0508.xml                             09-Jun-2021 08:29    3266
cvrf-CVE-2000-0573.xml                             09-Jun-2021 08:29    3413
cvrf-CVE-2000-0666.xml                             09-Jun-2021 08:29    3379
cvrf-CVE-2000-0800.xml                             09-Jun-2021 08:29    3351
cvrf-CVE-2000-0916.xml                             09-Jun-2021 08:29    3457
cvrf-CVE-2000-1254.xml                             02-Feb-2023 03:38    170K
cvrf-CVE-2001-0168.xml                             09-Jun-2021 08:29    3481
cvrf-CVE-2001-0328.xml                             09-Jun-2021 08:29    3538
cvrf-CVE-2001-0405.xml                             26-Nov-2022 03:04     74K
cvrf-CVE-2001-0554.xml                             09-Jun-2021 08:29    3513
cvrf-CVE-2001-0775.xml                             09-Jun-2021 08:29    3429
cvrf-CVE-2001-0851.xml                             26-Nov-2022 03:04     74K
cvrf-CVE-2001-1013.xml                             09-Jun-2021 08:29    3750
cvrf-CVE-2001-1267.xml                             18-Feb-2023 02:09     49K
cvrf-CVE-2001-1350.xml                             09-Jun-2021 08:29    3389
cvrf-CVE-2001-1483.xml                             09-Jun-2021 08:29    3528
cvrf-CVE-2001-1487.xml                             09-Jun-2021 08:29    3404
cvrf-CVE-2001-1593.xml                             20-Mar-2023 03:05    6041
cvrf-CVE-2002-0029.xml                             09-Jun-2021 08:30    4003
cvrf-CVE-2002-0389.xml                             15-Feb-2023 03:08    4764
cvrf-CVE-2002-0392.xml                             26-Nov-2022 03:04     36K
cvrf-CVE-2002-0399.xml                             02-Feb-2023 03:38     50K
cvrf-CVE-2002-0435.xml                             09-Jun-2021 08:30    3818
cvrf-CVE-2002-0510.xml                             09-Jun-2021 08:30    3440
cvrf-CVE-2002-0651.xml                             09-Jun-2021 08:30    3691
```

https://ftp.suse.com/pub/projects/security/cvrf-cve/

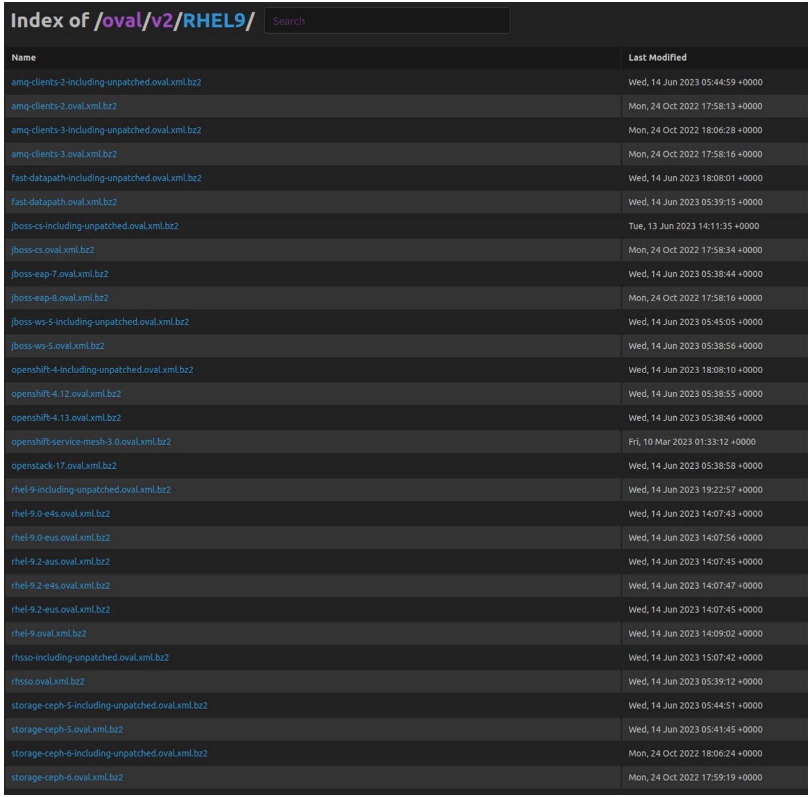
# 公開年やプロダクト毎でまとめる



## Index of /cvrf/

Search

| Name | Last Modified |
|---|---|
| 2000/ | - |
| 2001/ | - |
| 2002/ | - |
| 2003/ | - |
| 2004/ | - |
| 2005/ | - |
| 2006/ | - |
| 2007/ | - |
| 2008/ | - |
| 2009/ | - |
| 2010/ | - |
| 2011/ | - |
| 2012/ | - |
| 2013/ | - |
| 2014/ | - |
| 2015/ | - |
| 2016/ | - |
| 2017/ | - |
| 2018/ | - |
| 2019/ | - |
| 2020/ | - |
| 2021/ | - |
| 2022/ | - |
| 2023/ | - |



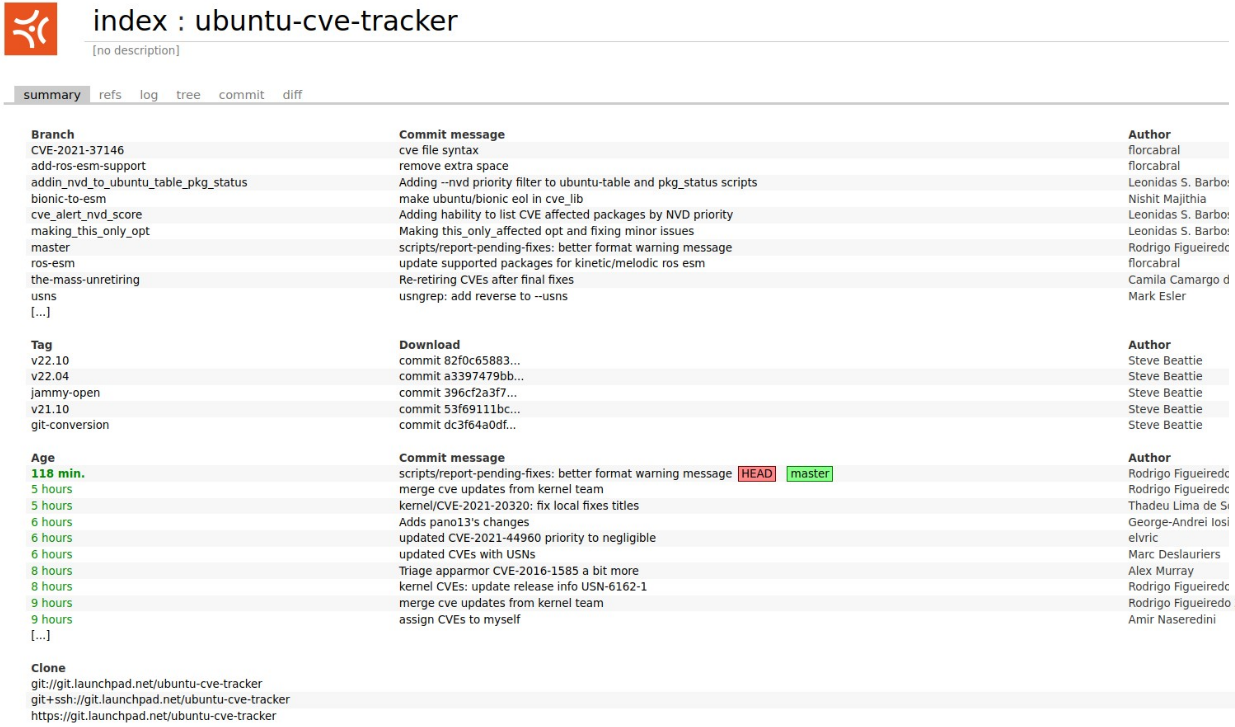
## Index of /oval/v2/RHEL9/

Search

| Name | Last Modified |
|---|---|
| amq-clients-2-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 05:44:59 +0000 |
| amq-clients-2.oval.xml.bz2 | Mon, 24 Oct 2022 17:58:13 +0000 |
| amq-clients-3-including-unpatched.oval.xml.bz2 | Mon, 24 Oct 2022 18:06:28 +0000 |
| amq-clients-3.oval.xml.bz2 | Mon, 24 Oct 2022 17:58:16 +0000 |
| fast-datapath-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 18:08:01 +0000 |
| fast-datapath.oval.xml.bz2 | Wed, 14 Jun 2023 05:39:15 +0000 |
| jboss-cs-including-unpatched.oval.xml.bz2 | Tue, 13 Jun 2023 14:11:35 +0000 |
| jboss-cs.oval.xml.bz2 | Mon, 24 Oct 2022 17:58:34 +0000 |
| jboss-eap-7.oval.xml.bz2 | Wed, 14 Jun 2023 05:38:44 +0000 |
| jboss-eap-8.oval.xml.bz2 | Mon, 24 Oct 2022 17:58:16 +0000 |
| jboss-ws-5-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 05:45:05 +0000 |
| jboss-ws-5.oval.xml.bz2 | Wed, 14 Jun 2023 05:38:56 +0000 |
| openshift-4-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 18:08:10 +0000 |
| openshift-4.12.oval.xml.bz2 | Wed, 14 Jun 2023 05:38:55 +0000 |
| openshift-4.13.oval.xml.bz2 | Wed, 14 Jun 2023 05:38:46 +0000 |
| openshift-service-mesh-3.0.oval.xml.bz2 | Fri, 10 Mar 2023 01:33:12 +0000 |
| openstack-17.oval.xml.bz2 | Wed, 14 Jun 2023 05:38:58 +0000 |
| rhel-9-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 19:22:57 +0000 |
| rhel-9.0-e4s.oval.xml.bz2 | Wed, 14 Jun 2023 14:07:43 +0000 |
| rhel-9.0-eus.oval.xml.bz2 | Wed, 14 Jun 2023 14:07:56 +0000 |
| rhel-9.2-aus.oval.xml.bz2 | Wed, 14 Jun 2023 14:07:45 +0000 |
| rhel-9.2-e4s.oval.xml.bz2 | Wed, 14 Jun 2023 14:07:47 +0000 |
| rhel-9.2-eus.oval.xml.bz2 | Wed, 14 Jun 2023 14:07:45 +0000 |
| rhel-9.oval.xml.bz2 | Wed, 14 Jun 2023 14:09:02 +0000 |
| rhsso-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 15:07:42 +0000 |
| rhsso.oval.xml.bz2 | Wed, 14 Jun 2023 05:39:12 +0000 |
| storage-ceph-5-including-unpatched.oval.xml.bz2 | Wed, 14 Jun 2023 05:44:51 +0000 |
| storage-ceph-5.oval.xml.bz2 | Wed, 14 Jun 2023 05:41:45 +0000 |
| storage-ceph-6-including-unpatched.oval.xml.bz2 | Mon, 24 Oct 2022 18:06:24 +0000 |
| storage-ceph-6.oval.xml.bz2 | Mon, 24 Oct 2022 17:59:19 +0000 |

[1] https://access.redhat.com/security/data/cvrf/ [2] https://www.redhat.com/security/data/oval/v2/RHEL9/

# Git Repository



index : ubuntu-cve-tracker

[no description]

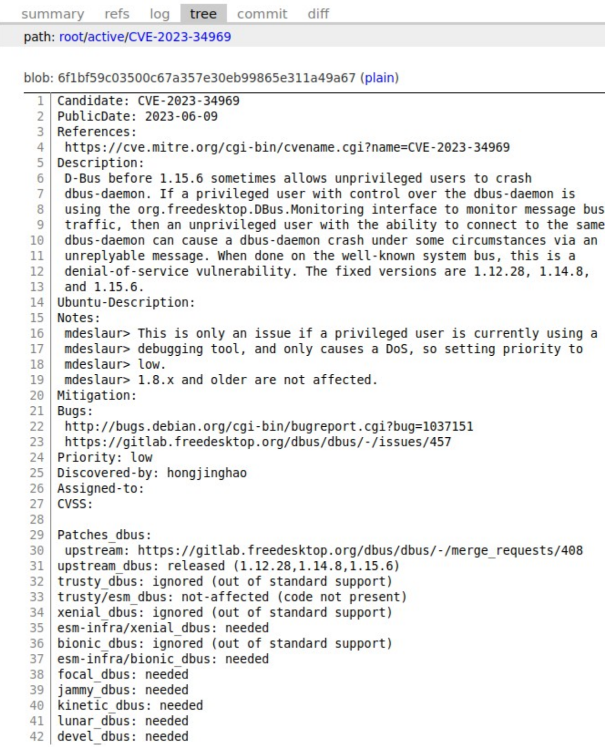
| Branch | Commit message | Author |
|---|---|---|
| CVE-2021-37146 | cve file syntax | florcabral |
| add-ros-esm-support | remove extra space | florcabral |
| addin_nvd_to_ubuntu_table_pkg_status | Adding --nvd priority filter to ubuntu-table and pkg_status scripts | Leonidas S. Barbo |
| bionic-to-esm | make ubuntu/bionic eol in cve_lib | Nishit Majithia |
| cve_alert_nvd_score | Adding hability to list CVE affected packages by NVD priority | Leonidas S. Barbo |
| making_this_only_opt | Making this_only_affected opt and fixing minor issues | Leonidas S. Barbo |
| master | scripts/report-pending-fixes: better format warning message | Rodrigo Figueiredo |
| ros-esm | update supported packages for kinetic/melodic ros esm | florcabral |
| the-mass-unretiring | Re-retiring CVEs after final fixes | Camila Camargo d |
| usns | usngrep: add reverse to --usns | Mark Esler |
| [...] | | |

| Tag | Download | Author |
|---|---|---|
| v22.10 | commit 82f0c65883... | Steve Beattie |
| v22.04 | commit a3397479bb... | Steve Beattie |
| jammy-open | commit 396cf2a3f7... | Steve Beattie |
| v21.10 | commit 53f69111bc... | Steve Beattie |
| git-conversion | commit dc3f64a0df... | Steve Beattie |

| Age | Commit message | Author |
|---|---|---|
| **118 min.** | scripts/report-pending-fixes: better format warning message HEAD master | Rodrigo Figueiredo |
| 5 hours | merge cve updates from kernel team | Rodrigo Figueiredo |
| 5 hours | kernel/CVE-2021-20320: fix local fixes titles | Thadeu Lima de S |
| 6 hours | Adds pano13's changes | George-Andrei Iosi |
| 6 hours | updated CVE-2021-44960 priority to negligible | elvric |
| 6 hours | updated CVEs with USNs | Marc Deslauriers |
| 8 hours | Triage apparmor CVE-2016-1585 a bit more | Alex Murray |
| 8 hours | kernel CVEs: update release info USN-6162-1 | Rodrigo Figueiredo |
| 9 hours | merge cve updates from kernel team | Rodrigo Figueiredo Zaiden |
| 9 hours | assign CVEs to myself | Amir Naseredini |
| [...] | | |

**Clone**

git://git.launchpad.net/ubuntu-cve-tracker
git+ssh://git.launchpad.net/ubuntu-cve-tracker
https://git.launchpad.net/ubuntu-cve-tracker



path: root/active/CVE-2023-34969

blob: 6f1bf59c03500c67a357e30eb99865e311a49a67 (plain)

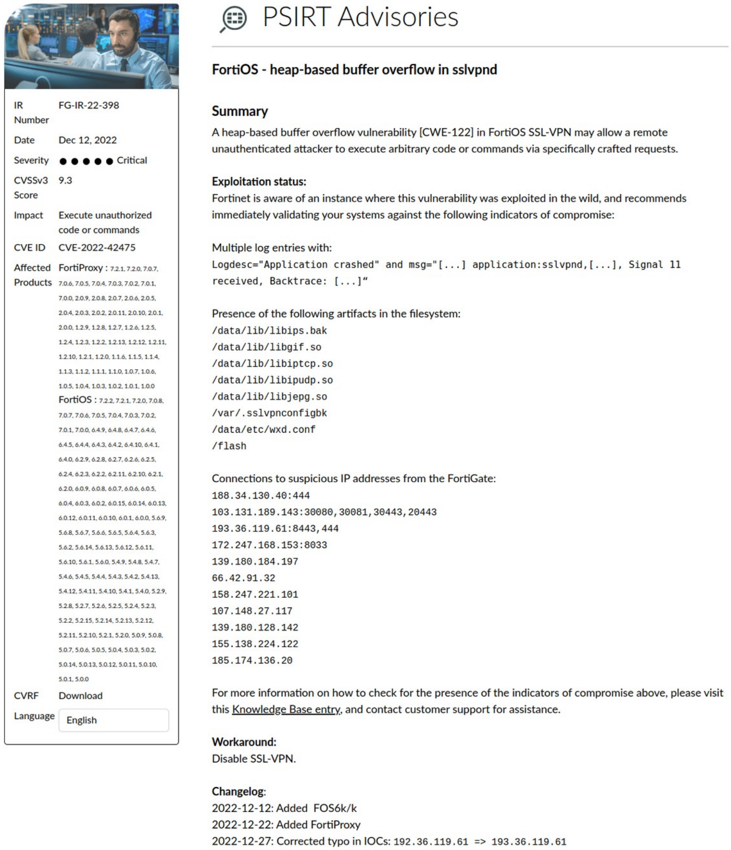
```
Candidate: CVE-2023-34969
PublicDate: 2023-06-09
References:
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34969
Description:
 D-Bus before 1.15.6 sometimes allows unprivileged users to crash
 dbus-daemon. If a privileged user with control over the dbus-daemon is
 using the org.freedesktop.DBus.Monitoring interface to monitor message bus
 traffic, then an unprivileged user with the ability to connect to the same
 dbus-daemon can cause a dbus-daemon crash under some circumstances via an
 unreplyable message. When done on the well-known system bus, this is a
 denial-of-service vulnerability. The fixed versions are 1.12.28, 1.14.8,
 and 1.15.6.
Ubuntu-Description:
Notes:
 mdeslaur> This is only an issue if a privileged user is currently using a
 mdeslaur> debugging tool, and only causes a DoS, so setting priority to
 mdeslaur> low.
 mdeslaur> 1.8.x and older are not affected.
Mitigation:
Bugs:
 http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1037151
 https://gitlab.freedesktop.org/dbus/dbus/-/issues/457
Priority: low
Discovered-by: hongjinghao
Assigned-to:
CVSS:

Patches_dbus:
 upstream: https://gitlab.freedesktop.org/dbus/dbus/-/merge_requests/408
upstream_dbus: released (1.12.28,1.14.8,1.15.6)
trusty_dbus: ignored (out of standard support)
trusty/esm_dbus: not-affected (code not present)
xenial_dbus: ignored (out of standard support)
esm-infra/xenial_dbus: needed
bionic_dbus: ignored (out of standard support)
esm-infra/bionic_dbus: needed
focal_dbus: needed
jammy_dbus: needed
kinetic_dbus: needed
lunar_dbus: needed
devel_dbus: needed
```

https://git.launchpad.net/ubuntu-cve-tracker/

# Appendix C:
# 困った脆弱性アドバイザリサンプル集

# NVD の情報が使えない

# 脆弱性アドバイザリの公開から NVD で取り込まれるまで、１ヶ月ほどかかる場合も



|  |  |
|---|---|
| IR Number | FG-IR-22-398 |
| Date | Dec 12, 2022 |
| Severity | ● ● ● ● ● Critical |
| CVSSv3 Score | 9.3 |
| Impact | Execute unauthorized code or commands |
| CVE ID | CVE-2022-42475 |
| Affected Products | FortiProxy : 7.2.1, 7.2.0, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 2.0.9, 2.0.8, 2.0.7, 2.0.6, 2.0.5, 2.0.4, 2.0.3, 2.0.2, 2.0.11, 2.0.10, 2.0.1, 2.0.0, 1.2.9, 1.2.8, 1.2.7, 1.2.6, 1.2.5, 1.2.4, 1.2.3, 1.2.2, 1.2.13, 1.2.12, 1.2.11, 1.2.10, 1.2.1, 1.2.0, 1.1.6, 1.1.5, 1.1.4, 1.1.3, 1.1.2, 1.1.1, 1.1.0, 1.0.7, 1.0.6, 1.0.5, 1.0.4, 1.0.3, 1.0.2, 1.0.1, 1.0.0<br>FortiOS : 7.2.2, 7.2.1, 7.2.0, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.10, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.11, 6.2.10, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.15, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0, 5.6.9, 5.6.8, 5.6.7, 5.6.6, 5.6.5, 5.6.4, 5.6.3, 5.6.2, 5.6.14, 5.6.13, 5.6.12, 5.6.11, 5.6.10, 5.6.1, 5.6.0, 5.4.9, 5.4.8, 5.4.7, 5.4.6, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.13, 5.4.12, 5.4.11, 5.4.10, 5.4.1, 5.4.0, 5.2.9, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.4, 5.2.3, 5.2.2, 5.2.15, 5.2.14, 5.2.13, 5.2.12, 5.2.11, 5.2.10, 5.2.1, 5.2.0, 5.0.9, 5.0.8, 5.0.7, 5.0.6, 5.0.5, 5.0.4, 5.0.3, 5.0.2, 5.0.14, 5.0.13, 5.0.12, 5.0.11, 5.0.10, 5.0.1, 5.0.0 |
| CVRF | Download |
| Language | English |

## PSIRT Advisories

### FortiOS - heap-based buffer overflow in sslvpnd

**Summary**

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

**Exploitation status:**
Fortinet is aware of an instance where this vulnerability was exploited in the wild, and recommends immediately validating your systems against the following indicators of compromise:

Multiple log entries with:

```
Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11
received, Backtrace: [...]"
```

Presence of the following artifacts in the filesystem:

```
/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/libipudp.so
/data/lib/libjepg.so
/var/.sslvpnconfigbk
/data/etc/wxd.conf
/flash
```

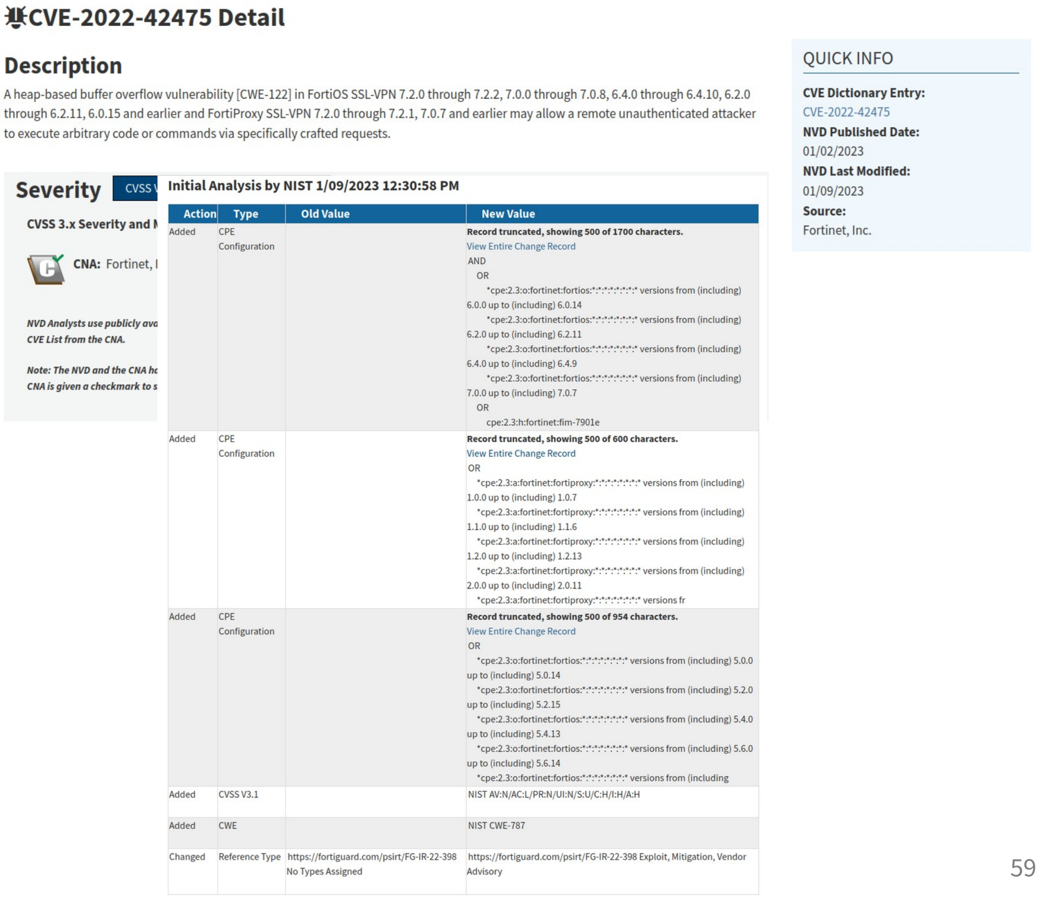
Connections to suspicious IP addresses from the FortiGate:

```
188.34.130.40:444
103.131.189.143:30080,30081,30443,20443
193.36.119.61:8443,444
172.247.168.153:8033
139.180.184.197
66.42.91.32
158.247.221.101
107.148.27.117
139.180.128.142
155.138.224.122
185.174.136.20
```

For more information on how to check for the presence of the indicators of compromise above, please visit this Knowledge Base entry, and contact customer support for assistance.

**Workaround:**
Disable SSL-VPN.

**Changelog:**
2022-12-12: Added FOS6k/k
2022-12-22: Added FortiProxy
2022-12-27: Corrected typo in IOCs: `192.36.119.61 => 193.36.119.61`



## CVE-2022-42475 Detail

### Description

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

### Severity

CVSS V

**CVSS 3.x Severity and M**

**CNA:** Fortinet, I

***NVD Analysts use publicly ava***
***CVE List from the CNA.***

***Note: The NVD and the CNA ha***
***CNA is given a checkmark to s***

**Initial Analysis by NIST 1/09/2023 12:30:58 PM**

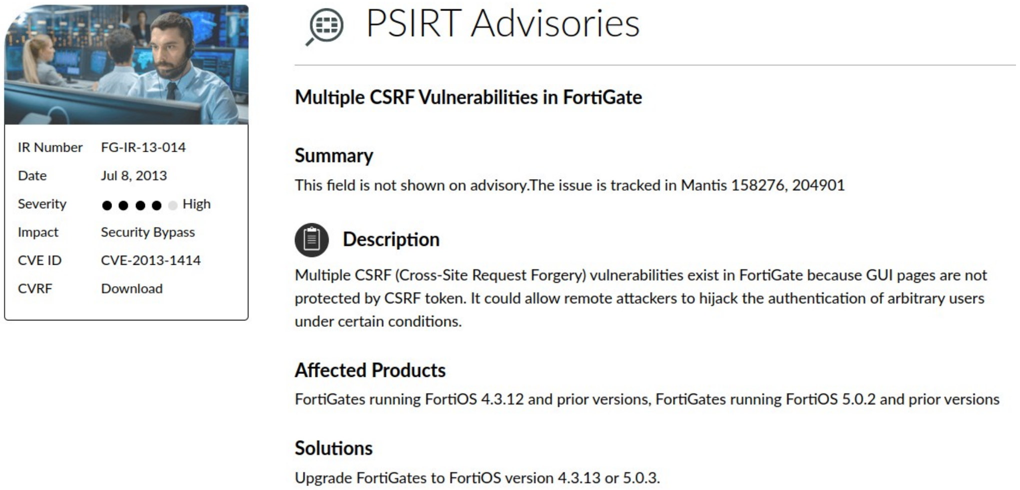
| Action | Type | Old Value | New Value |
|---|---|---|---|
| Added | CPE Configuration |  | **Record truncated, showing 500 of 1700 characters.**<br>View Entire Change Record<br>AND<br>OR<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 6.0.0 up to (including) 6.0.14<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 6.2.0 up to (including) 6.2.11<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 6.4.0 up to (including) 6.4.9<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 7.0.0 up to (including) 7.0.7<br>OR<br>cpe:2.3:h:fortinet:fim-7901e |
| Added | CPE Configuration |  | **Record truncated, showing 500 of 600 characters.**<br>View Entire Change Record<br>OR<br>*cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* versions from (including) 1.0.0 up to (including) 1.0.7<br>*cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* versions from (including) 1.1.0 up to (including) 1.1.6<br>*cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* versions from (including) 1.2.0 up to (including) 1.2.13<br>*cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* versions from (including) 2.0.0 up to (including) 2.0.11<br>*cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* versions fr |
| Added | CPE Configuration |  | **Record truncated, showing 500 of 954 characters.**<br>View Entire Change Record<br>OR<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 5.0.0 up to (including) 5.0.14<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 5.2.0 up to (including) 5.2.15<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 5.4.0 up to (including) 5.4.13<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including) 5.6.0 up to (including) 5.6.14<br>*cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* versions from (including |
| Added | CVSS V3.1 |  | NIST AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| Added | CWE |  | NIST CWE-787 |
| Changed | Reference Type | https://fortiguard.com/psirt/FG-IR-22-398 No Types Assigned | https://fortiguard.com/psirt/FG-IR-22-398 Exploit, Mitigation, Vendor Advisory |

**QUICK INFO**

**CVE Dictionary Entry:**
CVE-2022-42475
**NVD Published Date:**
01/02/2023
**NVD Last Modified:**
01/09/2023
**Source:**
Fortinet, Inc.

[1] https://www.fortiguard.com/psirt/FG-IR-22-398 [2] https://nvd.nist.gov/vuln/detail/CVE-2022-42475

# 脆弱性アドバイザリと NVD の間で影響するバージョンが異なる



| | |
|---|---|
| IR Number | FG-IR-13-014 |
| Date | Jul 8, 2013 |
| Severity | ●●●●○ High |
| Impact | Security Bypass |
| CVE ID | CVE-2013-1414 |
| CVRF | Download |

## PSIRT Advisories

### Multiple CSRF Vulnerabilities in FortiGate

**Summary**

This field is not shown on advisory.The issue is tracked in Mantis 158276, 204901

**Description**

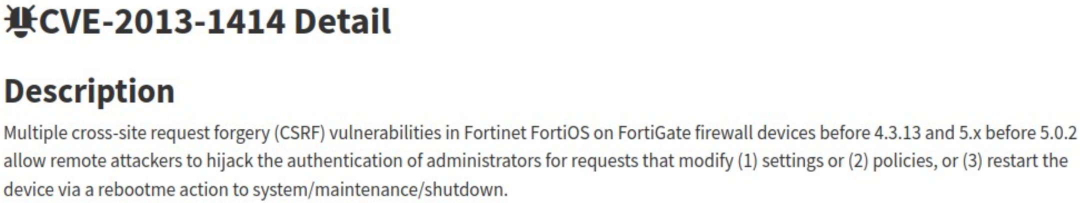
Multiple CSRF (Cross-Site Request Forgery) vulnerabilities exist in FortiGate because GUI pages are not protected by CSRF token. It could allow remote attackers to hijack the authentication of arbitrary users under certain conditions.

**Affected Products**

FortiGates running FortiOS 4.3.12 and prior versions, FortiGates running FortiOS 5.0.2 and prior versions

**Solutions**

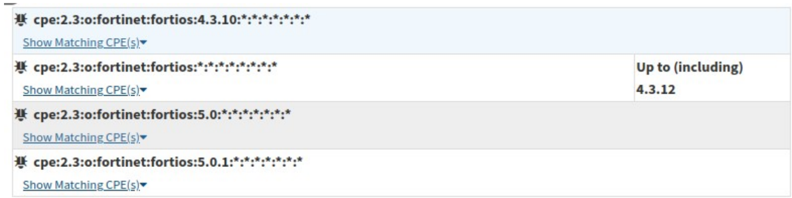
Upgrade FortiGates to FortiOS version 4.3.13 or 5.0.3.



## CVE-2013-1414 Detail

### Description

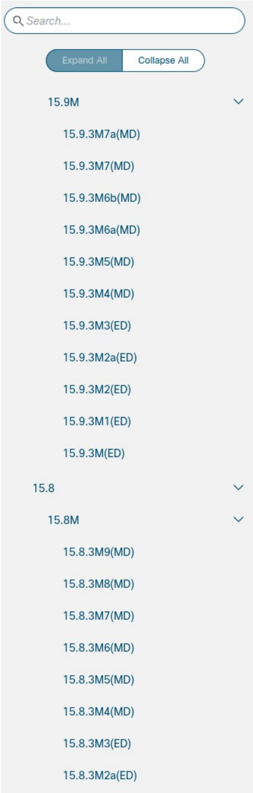
Multiple cross-site request forgery (CSRF) vulnerabilities in Fortinet FortiOS on FortiGate firewall devices before 4.3.13 and 5.x before 5.0.2 allow remote attackers to hijack the authentication of administrators for requests that modify (1) settings or (2) policies, or (3) restart the device via a rebootme action to system/maintenance/shutdown.



| | |
|---|---|
| cpe:2.3:o:fortinet:fortios:4.3.10:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | |
| cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | Up to (including)<br>4.3.12 |
| cpe:2.3:o:fortinet:fortios:5.0:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | |
| cpe:2.3:o:fortinet:fortios:5.0.1:*:*:*:*:*:*:*<br>Show Matching CPE(s)▾ | |

[1] https://www.fortiguard.com/psirt/FG-IR-13-014 [2] https://nvd.nist.gov/vuln/detail/CVE-2013-1414

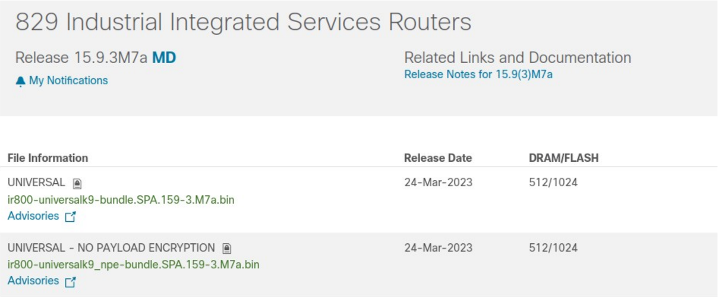
NVDの15.9(3)未満は15.8(3)m9などを指しているはずが、15.8(3)m9などのレンジに対応するCPEが見つからない（= NVDではCisco IOS向けのバージョン比較が用意されていないため、すべて列挙するしかない



Search...

Expand All | Collapse All

- 15.9M
  - 15.9.3M7a(MD)
  - 15.9.3M7(MD)
  - 15.9.3M6b(MD)
  - 15.9.3M6a(MD)
  - 15.9.3M5(MD)
  - 15.9.3M4(MD)
  - 15.9.3M3(ED)
  - 15.9.3M2a(ED)
  - 15.9.3M2(ED)
  - 15.9.3M1(ED)
  - 15.9.3M(ED)
- 15.8
- 15.8M
  - 15.8.3M9(MD)
  - 15.8.3M8(MD)
  - 15.8.3M7(MD)
  - 15.8.3M6(MD)
  - 15.8.3M5(MD)
  - 15.8.3M4(MD)
  - 15.8.3M3(ED)
  - 15.8.3M2a(ED)



829 Industrial Integrated Services Routers

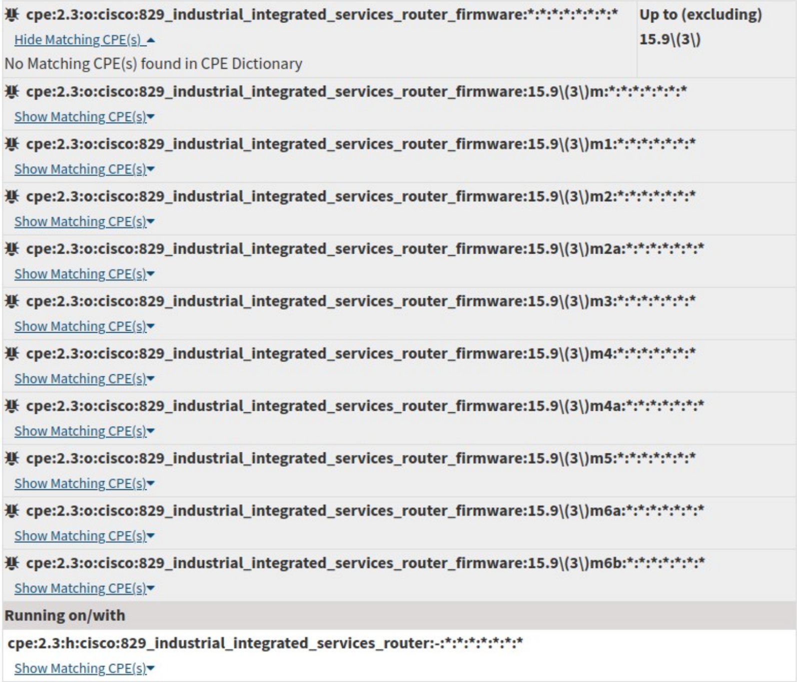
Release 15.9.3M7a **MD**

My Notifications

Related Links and Documentation

Release Notes for 15.9(3)M7a

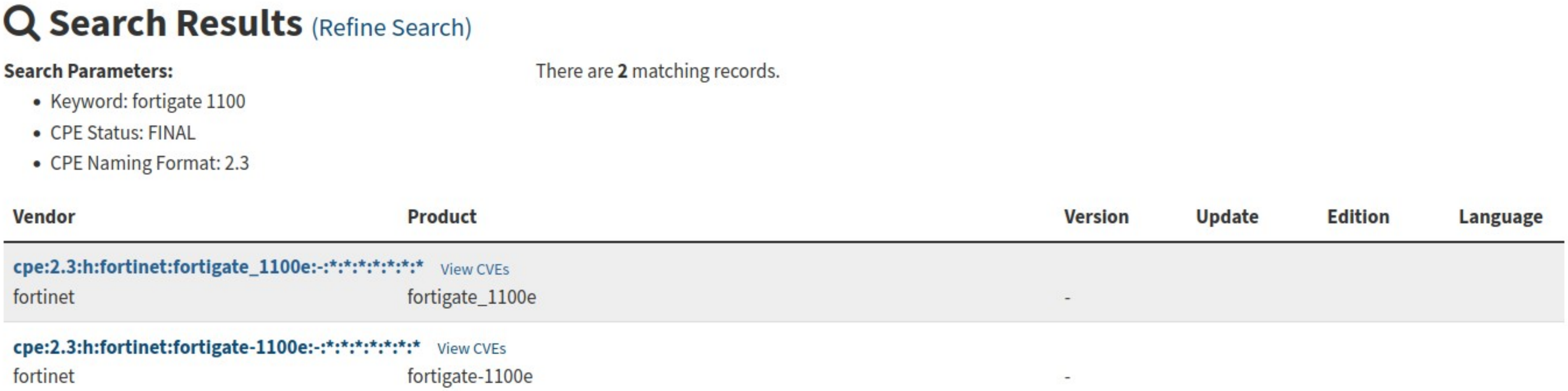
| File Information | Release Date | DRAM/FLASH |
|---|---|---|
| UNIVERSAL<br>ir800-universalk9-bundle.SPA.159-3.M7a.bin<br>Advisories | 24-Mar-2023 | 512/1024 |
| UNIVERSAL - NO PAYLOAD ENCRYPTION<br>ir800-universalk9_npe-bundle.SPA.159-3.M7a.bin<br>Advisories | 24-Mar-2023 | 512/1024 |



| | |
|---|---|
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:*:*:*:*:*:*:*:***<br>Hide Matching CPE(s) ▲<br>No Matching CPE(s) found in CPE Dictionary | **Up to (excluding)<br>15.9\(3\)** |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m1:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m2:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m2a:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m3:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m4:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m4a:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m5:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m6a:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **cpe:2.3:o:cisco:829_industrial_integrated_services_router_firmware:15.9\(3\)m6b:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |
| **Running on/with** | |
| **cpe:2.3:h:cisco:829_industrial_integrated_services_router:-:*:*:*:*:*:*:***<br>Show Matching CPE(s)▾ | |

[1] https://software.cisco.com/download/home/286287074/type/280805680/release/15.9.3M7a [2] https://nvd.nist.gov/vuln/detail/CVE-2023-20076

# 同じ製品を指す表現が複数ある



## Search Results (Refine Search)

**Search Parameters:**

- Keyword: fortigate 1100
- CPE Status: FINAL
- CPE Naming Format: 2.3

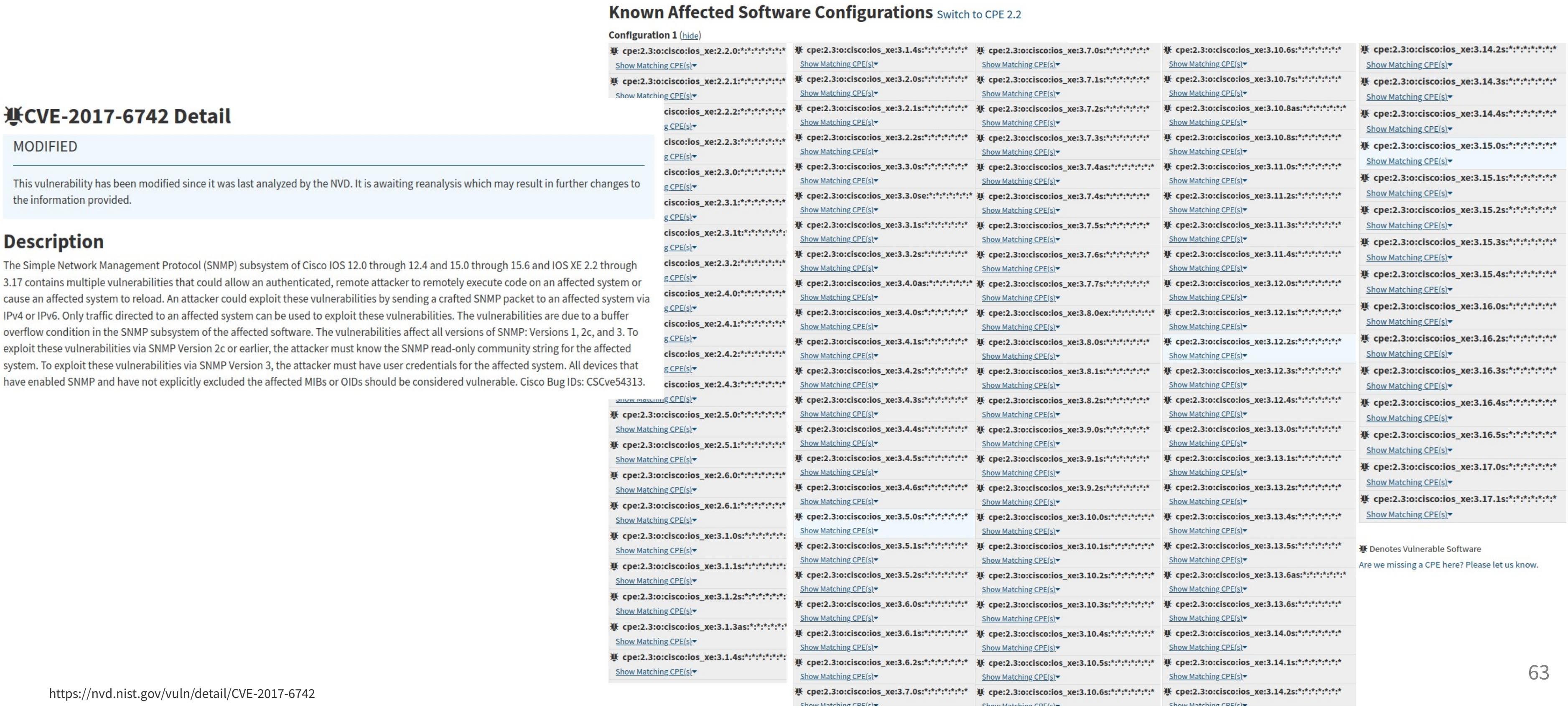
There are **2** matching records.

| Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|
| **cpe:2.3:h:fortinet:fortigate_1100e:-:*:*:*:*:*:*:*** View CVEs | | | | | |
| fortinet | fortigate_1100e | - | | | |
| **cpe:2.3:h:fortinet:fortigate-1100e:-:*:*:*:*:*:*:*** View CVEs | | | | | |
| fortinet | fortigate-1100e | - | | | |

https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=fortigate+1100

Description の記述と影響あるソフトウェアの列挙が異なる

Description によると IOS と IOS XE に影響するようだが、IOS XE のみ列挙されている



## CVE-2017-6742 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Description

The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve54313.

### Known Affected Software Configurations Switch to CPE 2.2

**Configuration 1** (hide)

```
cpe:2.3:o:cisco:ios_xe:2.2.0:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:2.2.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cisco:ios_xe:2.2.2:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.2.3:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.3.0:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.3.1:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.3.1t:*:*:*:*:*:*:
g CPE(s)▾
cisco:ios_xe:2.3.2:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.4.0:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.4.1:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.4.2:*:*:*:*:*:*:*
g CPE(s)▾
cisco:ios_xe:2.4.3:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:2.5.0:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:2.5.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:2.6.0:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:2.6.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.0s:*:*:*:*:*:*:
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.1s:*:*:*:*:*:*:
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.2s:*:*:*:*:*:*:
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.3as:*:*:*:*:*:
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.4s:*:*:*:*:*:*:
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.1.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.2.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.2.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.2.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.3.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.3.0se:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.3.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.3.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.0as:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.5s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.4.6s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.5.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.5.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.5.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.6.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.6.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.6.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.4as:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.5s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.6s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.7.7s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.8.0ex:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.8.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.8.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.8.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.9.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.9.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.9.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.5s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.6s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.6s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.7s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.8as:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.10.8s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.11.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.11.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.11.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.11.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.12.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.12.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.12.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.12.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.12.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.5s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.6as:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.13.6s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.14.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.15.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.15.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.15.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.15.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.15.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.16.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.16.2s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.16.3s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.16.4s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.16.5s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.17.0s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
cpe:2.3:o:cisco:ios_xe:3.17.1s:*:*:*:*:*:*:*
Show Matching CPE(s)▾
```

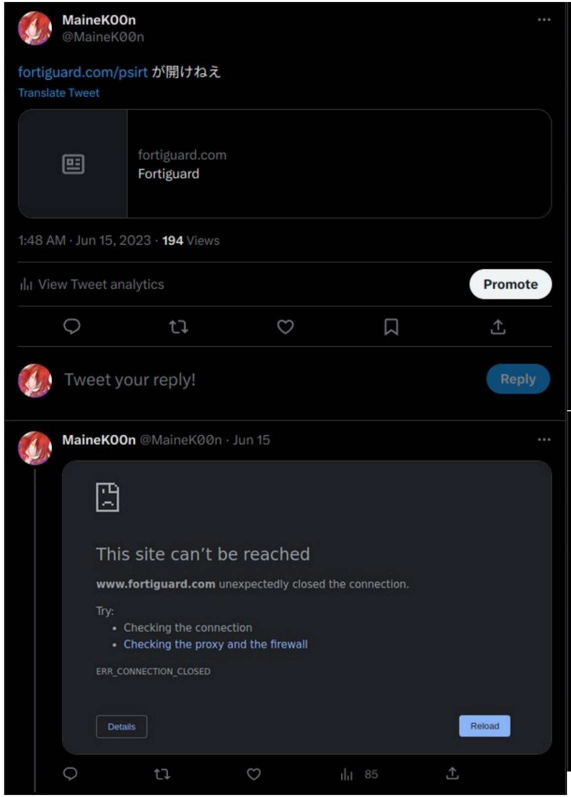
Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

https://nvd.nist.gov/vuln/detail/CVE-2017-6742

# 脆弱性アドバイザリへのアクセス

# 脆弱性アドバイザリへ安定的にアクセスできない



MaineK0On
@MaineK00n

fortiguard.com/psirt が開けねえ
Translate Tweet

fortiguard.com
Fortiguard

1:48 AM · Jun 15, 2023 · **194** Views

MaineK0On @MaineK00n · Jun 15

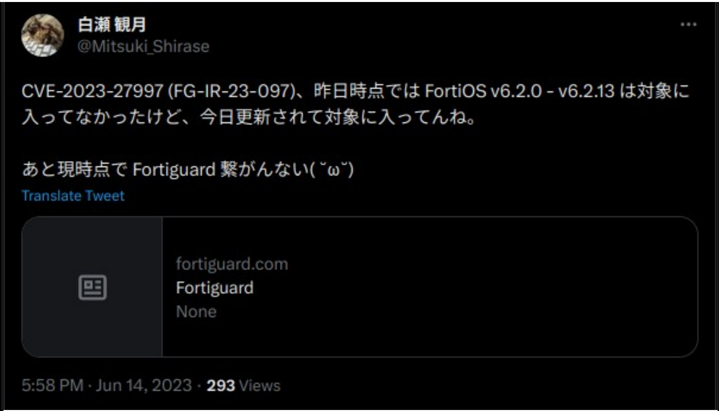
This site can't be reached

**www.fortiguard.com** unexpectedly closed the connection.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_CLOSED



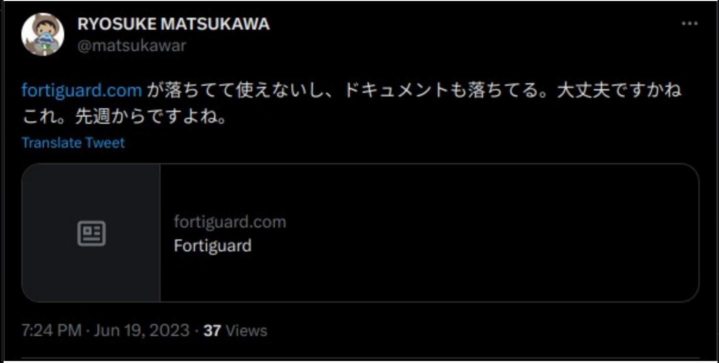
白瀬 観月
@Mitsuki_Shirase

CVE-2023-27997 (FG-IR-23-097)、昨日時点では FortiOS v6.2.0 - v6.2.13 は対象に入ってなかったけど、今日更新されて対象に入ってんね。

あと現時点で Fortiguard 繋がんない(˘ω˘)
Translate Tweet

fortiguard.com
Fortiguard
None

5:58 PM · Jun 14, 2023 · **293** Views

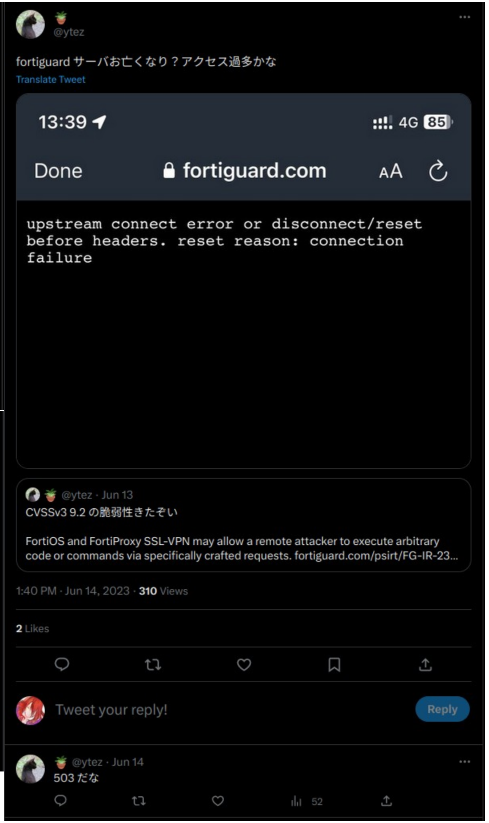


RYOSUKE MATSUKAWA
@matsukawar

fortiguard.com が落ちてて使えないし、ドキュメントも落ちてる。大丈夫ですかねこれ。先週からですよね。
Translate Tweet

fortiguard.com
Fortiguard

7:24 PM · Jun 19, 2023 · **37** Views



@ytez

fortiguard サーバお亡くなり？アクセス過多かな
Translate Tweet

```
upstream connect error or disconnect/reset
before headers. reset reason: connection
failure
```

@ytez · Jun 13
CVSSv3 9.2 の脆弱性きたぞい

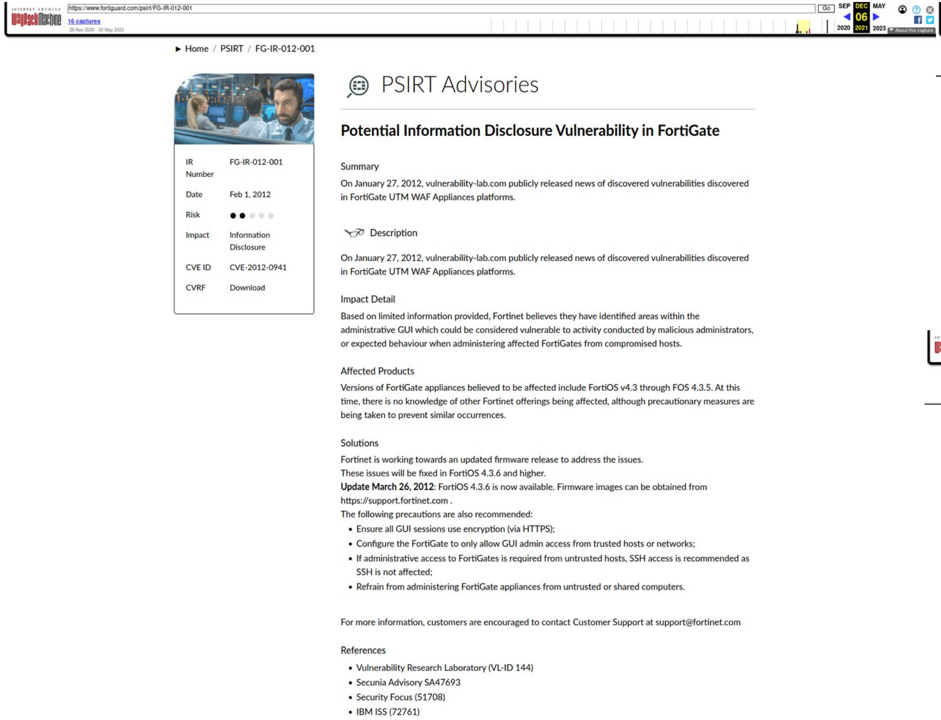
FortiOS and FortiProxy SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests. fortiguard.com/psirt/FG-IR-23...

1:40 PM · Jun 14, 2023 · **310** Views

**2** Likes

@ytez · Jun 14
503 だな

# 脆弱性アドバイザリがエラーでアクセスできない



▸ Home / PSIRT / FG-IR-012-001

## PSIRT Advisories

| | |
|---|---|
| IR Number | FG-IR-012-001 |
| Date | Feb 1, 2012 |
| Risk | ●●○○○ |
| Impact | Information Disclosure |
| CVE ID | CVE-2012-0941 |
| CVRF | Download |

### Potential Information Disclosure Vulnerability in FortiGate

Summary

On January 27, 2012, vulnerability-lab.com publicly released news of discovered vulnerabilities discovered in FortiGate UTM WAF Appliances platforms.

Description

On January 27, 2012, vulnerability-lab.com publicly released news of discovered vulnerabilities discovered in FortiGate UTM WAF Appliances platforms.

Impact Detail

Based on limited information provided, Fortinet believes they have identified areas within the administrative GUI which could be considered vulnerable to activity conducted by malicious administrators, or expected behaviour when administering affected FortiGates from compromised hosts.

Affected Products

Versions of FortiGate appliances believed to be affected include FortiOS v4.3 through FOS 4.3.5. At this time, there is no knowledge of other Fortinet offerings being affected, although precautionary measures are being taken to prevent similar occurrences.

Solutions

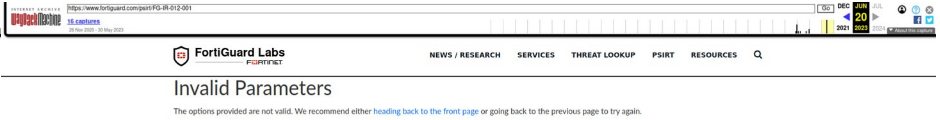
Fortinet is working towards an updated firmware release to address the issues.
These issues will be fixed in FortiOS 4.3.6 and higher.
**Update March 26, 2012**: FortiOS 4.3.6 is now available. Firmware images can be obtained from https://support.fortinet.com .
The following precautions are also recommended:

- Ensure all GUI sessions use encryption (via HTTPS);
- Configure the FortiGate to only allow GUI admin access from trusted hosts or networks;
- If administrative access to FortiGates is required from untrusted hosts, SSH access is recommended as SSH is not affected;
- Refrain from administering FortiGate appliances from untrusted or shared computers.

For more information, customers are encouraged to contact Customer Support at support@fortinet.com

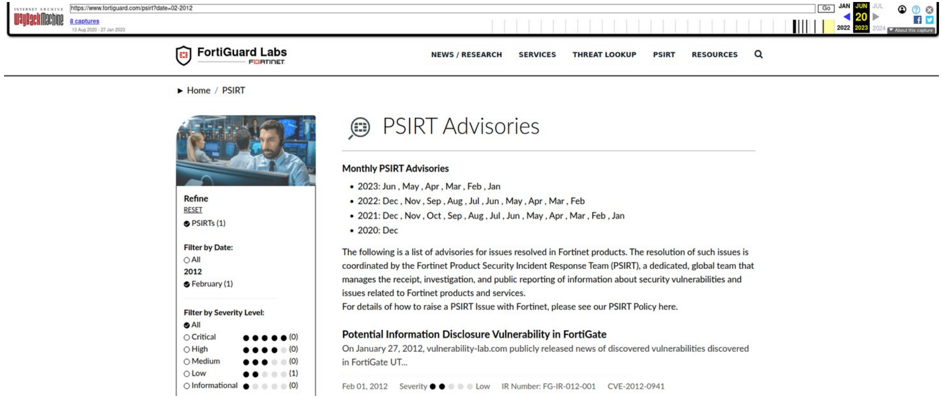
References

- Vulnerability Research Laboratory (VL-ID 144)
- Secunia Advisory SA47693
- Security Focus (51708)
- IBM ISS (72761)



## Invalid Parameters

The options provided are not valid. We recommend either heading back to the front page or going back to the previous page to try again.



▸ Home / PSIRT

## PSIRT Advisories

Refine
RESET
● PSIRTs (1)

Filter by Date:
○ All
2012
● February (1)

Filter by Severity Level:
● All
○ Critical ●●●●● (0)
○ High ●●●●○ (0)
○ Medium ●●●○○ (0)
○ Low ●●○○○ (1)
○ Informational ●○○○○ (0)

Monthly PSIRT Advisories

- 2023: Jun , May , Apr , Mar , Feb , Jan
- 2022: Dec , Nov , Sep , Aug , Jul , Jun , May , Apr , Mar , Feb
- 2021: Dec , Nov , Oct , Sep , Aug , Jul , Jun , May , Apr , Mar , Feb , Jan
- 2020: Dec

The following is a list of advisories for issues resolved in Fortinet products. The resolution of such issues is coordinated by the Fortinet Product Security Incident Response Team (PSIRT), a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Fortinet products and services.
For details of how to raise a PSIRT Issue with Fortinet, please see our PSIRT Policy here.

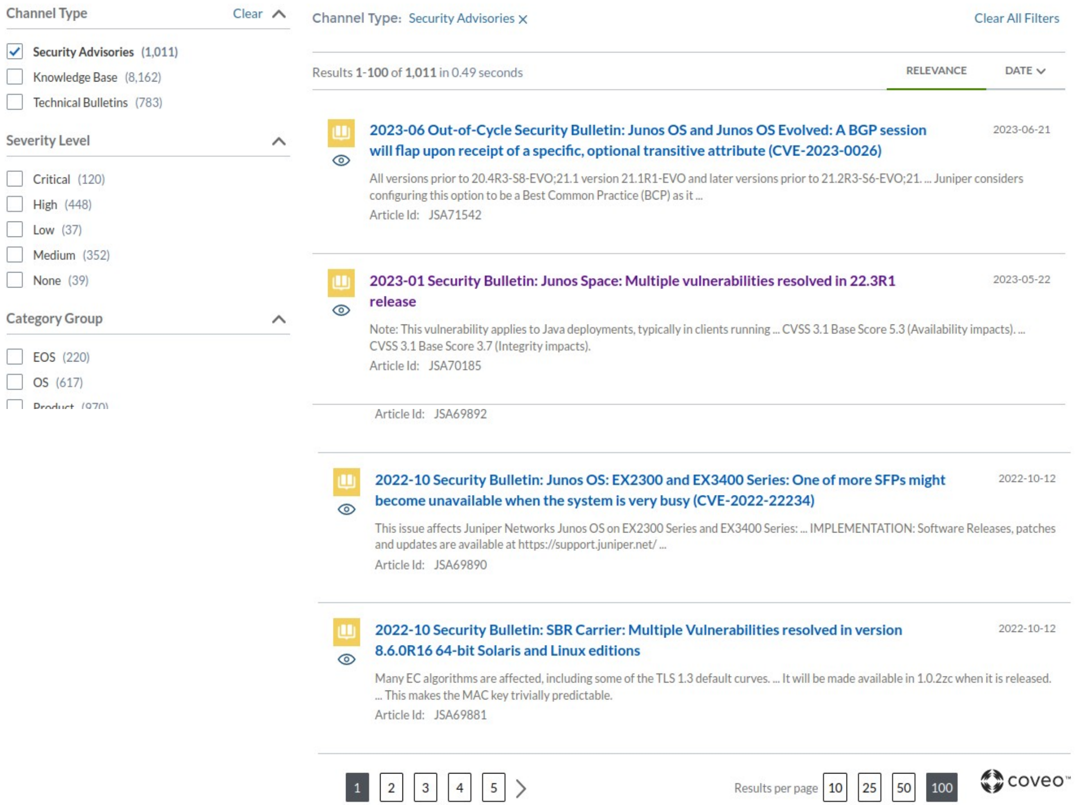
### Potential Information Disclosure Vulnerability in FortiGate

On January 27, 2012, vulnerability-lab.com publicly released news of discovered vulnerabilities discovered in FortiGate UT...

Feb 01, 2012 Severity ●●○○○ Low IR Number: FG-IR-012-001 CVE-2012-0941

[1] http://web.archive.org/web/20211206170652/https://www.fortiguard.com/psirt/FG-IR-012-001 [2] http://web.archive.org/web/20230620045853/https://www.fortiguard.com/psirt/FG-IR-012-001
[3] http://web.archive.org/web/20230620050517/https://www.fortiguard.com/psirt?date=02-2012

# 定期的な取得とページネーションの相性が悪い



Channel Type　Clear

☑ Security Advisories (1,011)
□ Knowledge Base (8,162)
□ Technical Bulletins (783)

Severity Level

□ Critical (120)
□ High (448)
□ Low (37)
□ Medium (352)
□ None (39)

Category Group

□ EOS (220)
□ OS (617)
□ Product (970)

Channel Type: Security Advisories ✕　Clear All Filters

Results **1-100** of **1,011** in 0.49 seconds　RELEVANCE　DATE

**2023-06 Out-of-Cycle Security Bulletin: Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026)**　2023-06-21

All versions prior to 20.4R3-S8-EVO;21.1 version 21.1R1-EVO and later versions prior to 21.2R3-S6-EVO;21. ... Juniper considers configuring this option to be a Best Common Practice (BCP) as it ...

Article Id: JSA71542

**2023-01 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 22.3R1 release**　2023-05-22

Note: This vulnerability applies to Java deployments, typically in clients running ... CVSS 3.1 Base Score 5.3 (Availability impacts). ... CVSS 3.1 Base Score 3.7 (Integrity impacts).

Article Id: JSA70185

Article Id: JSA69892

**2022-10 Security Bulletin: Junos OS: EX2300 and EX3400 Series: One of more SFPs might become unavailable when the system is very busy (CVE-2022-22234)**　2022-10-12

This issue affects Juniper Networks Junos OS on EX2300 Series and EX3400 Series: ... IMPLEMENTATION: Software Releases, patches and updates are available at https://support.juniper.net/ ...

Article Id: JSA69890

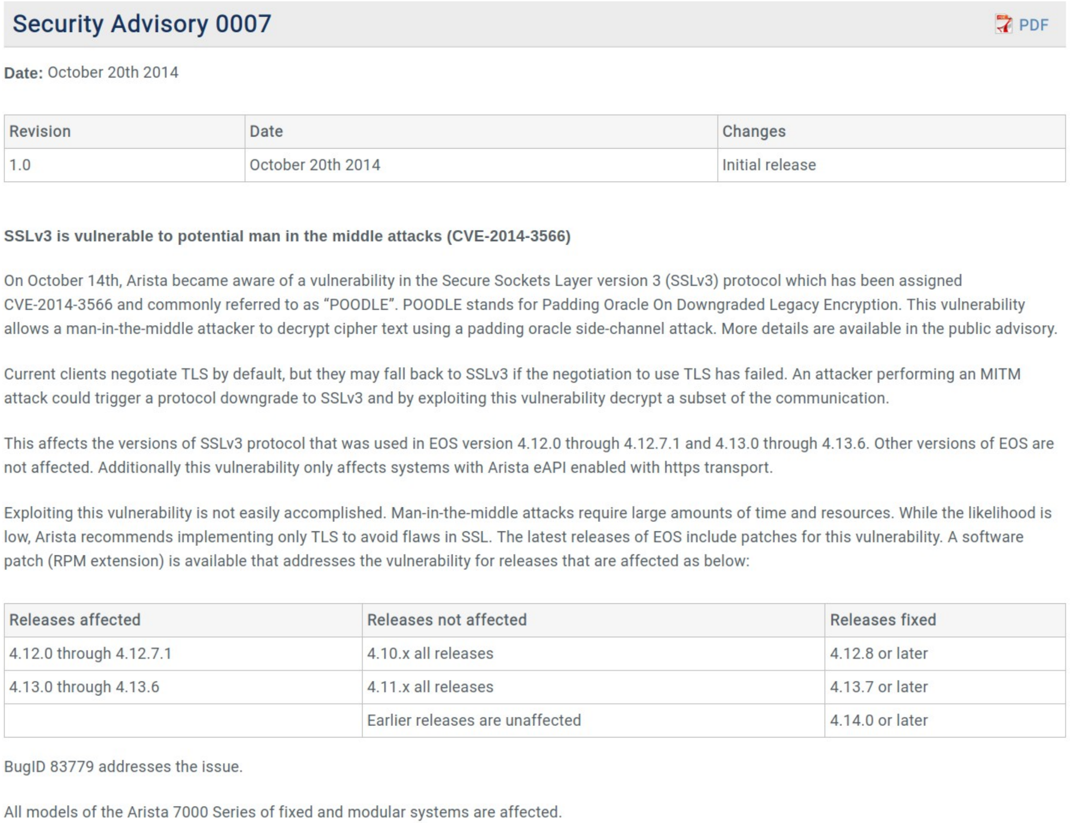
**2022-10 Security Bulletin: SBR Carrier: Multiple Vulnerabilities resolved in version 8.6.0R16 64-bit Solaris and Linux editions**　2022-10-12

Many EC algorithms are affected, including some of the TLS 1.3 default curves. ... It will be made available in 1.0.2zc when it is released. ... This makes the MAC key trivially predictable.

Article Id: JSA69881

https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&numberOfResults=100&f:ctype=[Security%20Advisories]

# HTML や PDF のみの提供のため、安定した情報収集が難しい



## Security Advisory 0007

PDF

**Date:** October 20th 2014

| Revision | Date | Changes |
|---|---|---|
| 1.0 | October 20th 2014 | Initial release |

**SSLv3 is vulnerable to potential man in the middle attacks (CVE-2014-3566)**

On October 14th, Arista became aware of a vulnerability in the Secure Sockets Layer version 3 (SSLv3) protocol which has been assigned CVE-2014-3566 and commonly referred to as “POODLE”. POODLE stands for Padding Oracle On Downgraded Legacy Encryption. This vulnerability allows a man-in-the-middle attacker to decrypt cipher text using a padding oracle side-channel attack. More details are available in the public advisory.

Current clients negotiate TLS by default, but they may fall back to SSLv3 if the negotiation to use TLS has failed. An attacker performing an MITM attack could trigger a protocol downgrade to SSLv3 and by exploiting this vulnerability decrypt a subset of the communication.

This affects the versions of SSLv3 protocol that was used in EOS version 4.12.0 through 4.12.7.1 and 4.13.0 through 4.13.6. Other versions of EOS are not affected. Additionally this vulnerability only affects systems with Arista eAPI enabled with https transport.

Exploiting this vulnerability is not easily accomplished. Man-in-the-middle attacks require large amounts of time and resources. While the likelihood is low, Arista recommends implementing only TLS to avoid flaws in SSL. The latest releases of EOS include patches for this vulnerability. A software patch (RPM extension) is available that addresses the vulnerability for releases that are affected as below:

| Releases affected | Releases not affected | Releases fixed |
|---|---|---|
| 4.12.0 through 4.12.7.1 | 4.10.x all releases | 4.12.8 or later |
| 4.13.0 through 4.13.6 | 4.11.x all releases | 4.13.7 or later |
|  | Earlier releases are unaffected | 4.14.0 or later |

BugID 83779 addresses the issue.

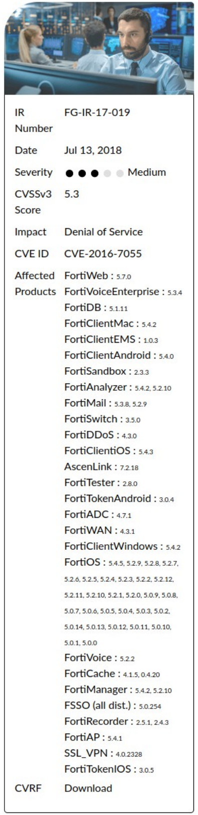
All models of the Arista 7000 Series of fixed and modular systems are affected.

https://www.arista.com/en/support/advisories-notices/security-advisory/1015-security-advisory-7

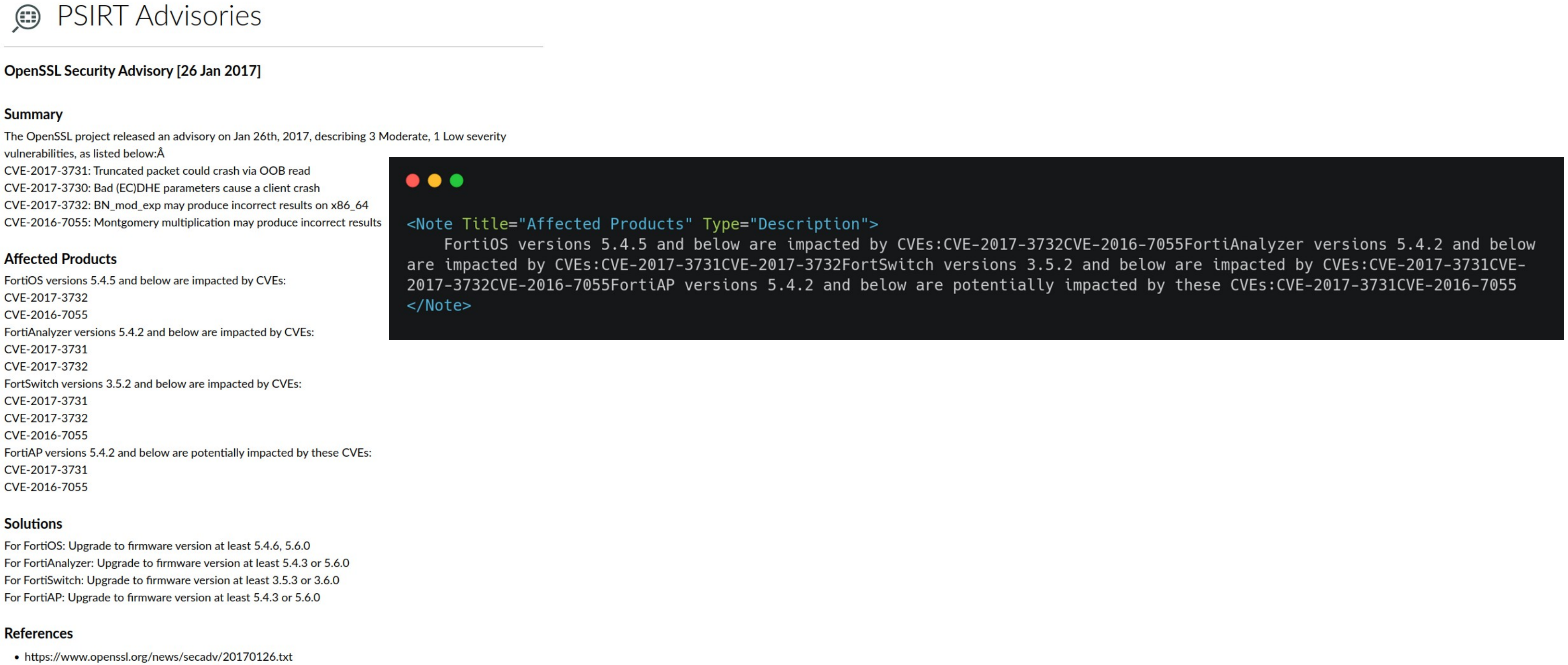
# 脆弱性アドバイザリの表現・解釈

# Web 版と CVRF/CSAF で記述が異なる

CVRF （= Web 版 アドバイザリ本文）にはないプロダクトが Web 版サイドバーで列挙されている



| | |
|---|---|
| IR Number | FG-IR-17-019 |
| Date | Jul 13, 2018 |
| Severity | ●●●○○ Medium |
| CVSSv3 Score | 5.3 |
| Impact | Denial of Service |
| CVE ID | CVE-2016-7055 |
| Affected Products | FortiWeb : 5.7.0<br>FortiVoiceEnterprise : 5.3.4<br>FortiDB : 5.1.11<br>FortiClientMac : 5.4.2<br>FortiClientEMS : 1.0.3<br>FortiClientAndroid : 5.4.0<br>FortiSandbox : 2.3.3<br>FortiAnalyzer : 5.4.2, 5.2.10<br>FortiMail : 5.3.8, 5.2.9<br>FortiSwitch : 3.5.0<br>FortiDDoS : 4.3.0<br>FortiClientiOS : 5.4.3<br>AscenLink : 7.2.18<br>FortiTester : 2.8.0<br>FortiTokenAndroid : 3.0.4<br>FortiADC : 4.7.1<br>FortiWAN : 4.3.1<br>FortiClientWindows : 5.4.2<br>FortiOS : 5.4.5, 5.2.9, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.4, 5.2.3, 5.2.2, 5.2.12, 5.2.11, 5.2.10, 5.2.1, 5.2.0, 5.0.9, 5.0.8, 5.0.7, 5.0.6, 5.0.5, 5.0.4, 5.0.3, 5.0.2, 5.0.14, 5.0.13, 5.0.12, 5.0.11, 5.0.10, 5.0.1, 5.0.0<br>FortiVoice : 5.2.2<br>FortiCache : 4.1.5, 0.4.20<br>FortiManager : 5.4.2, 5.2.10<br>FSSO (all dist.) : 5.0.254<br>FortiRecorder : 2.5.1, 2.4.3<br>FortiAP : 5.4.1<br>SSL_VPN : 4.0.2328<br>FortiTokenIOS : 3.0.5 |
| CVRF | Download |



## PSIRT Advisories

**OpenSSL Security Advisory [26 Jan 2017]**

**Summary**

The OpenSSL project released an advisory on Jan 26th, 2017, describing 3 Moderate, 1 Low severity vulnerabilities, as listed below:Â
CVE-2017-3731: Truncated packet could crash via OOB read
CVE-2017-3730: Bad (EC)DHE parameters cause a client crash
CVE-2017-3732: BN_mod_exp may produce incorrect results on x86_64
CVE-2016-7055: Montgomery multiplication may produce incorrect results

**Affected Products**

FortiOS versions 5.4.5 and below are impacted by CVEs:
CVE-2017-3732
CVE-2016-7055
FortiAnalyzer versions 5.4.2 and below are impacted by CVEs:
CVE-2017-3731
CVE-2017-3732
FortSwitch versions 3.5.2 and below are impacted by CVEs:
CVE-2017-3731
CVE-2017-3732
CVE-2016-7055
FortiAP versions 5.4.2 and below are potentially impacted by these CVEs:
CVE-2017-3731
CVE-2016-7055

**Solutions**

For FortiOS: Upgrade to firmware version at least 5.4.6, 5.6.0
For FortiAnalyzer: Upgrade to firmware version at least 5.4.3 or 5.6.0
For FortiSwitch: Upgrade to firmware version at least 3.5.3 or 3.6.0
For FortiAP: Upgrade to firmware version at least 5.4.3 or 5.6.0

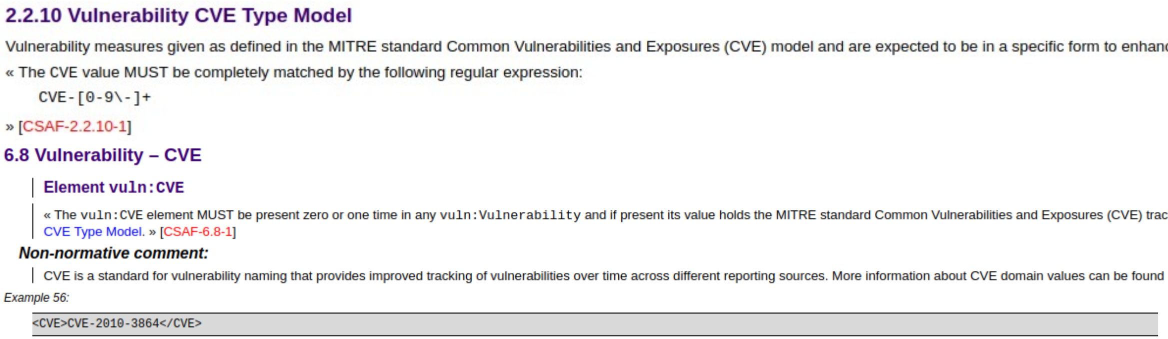
**References**

- https://www.openssl.org/news/secadv/20170126.txt

```
<Note Title="Affected Products" Type="Description">
    FortiOS versions 5.4.5 and below are impacted by CVEs:CVE-2017-3732CVE-2016-7055FortiAnalyzer versions 5.4.2 and below
are impacted by CVEs:CVE-2017-3731CVE-2017-3732FortSwitch versions 3.5.2 and below are impacted by CVEs:CVE-2017-3731CVE-
2017-3732CVE-2016-7055FortiAP versions 5.4.2 and below are potentially impacted by these CVEs:CVE-2017-3731CVE-2016-7055
</Note>
```

[1] https://www.fortiguard.com/psirt/FG-IR-17-019 [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-17-019

# CVRF/CSAF の仕様を満たしていない (e.g. 1 vulnerability : n CVE になっている



### 2.2.10 Vulnerability CVE Type Model

Vulnerability measures given as defined in the MITRE standard Common Vulnerabilities and Exposures (CVE) model and are expected to be in a specific form to enhance interoperability.

« The CVE value MUST be completely matched by the following regular expression:

```
CVE-[0-9\-]+
```

» [CSAF-2.2.10-1]

### 6.8 Vulnerability – CVE

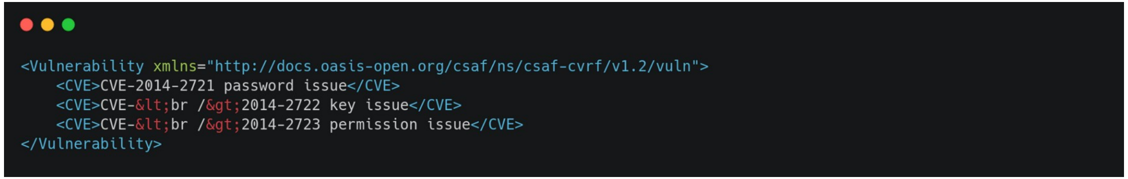
> **Element `vuln:CVE`**
>
> « The `vuln:CVE` element MUST be present zero or one time in any `vuln:Vulnerability` and if present its value holds the MITRE standard Common Vulnerabilities and Exposures (CVE) tracking number for the vulnerability and this value MUST match the pattern documented in section 2.2.10 Vulnerability CVE Type Model. » [CSAF-6.8-1]

***Non-normative comment:***

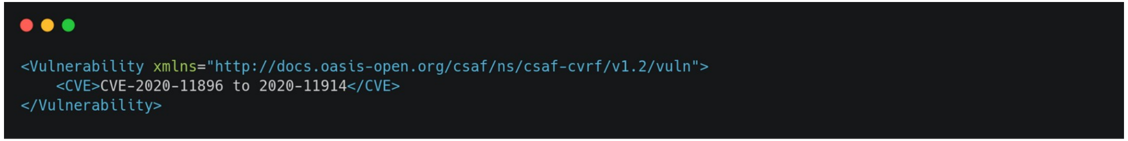
> CVE is a standard for vulnerability naming that provides improved tracking of vulnerabilities over time across different reporting sources. More information about CVE domain values can be found in section 2.2.10 Vulnerability CVE Type Model.

*Example 56:*

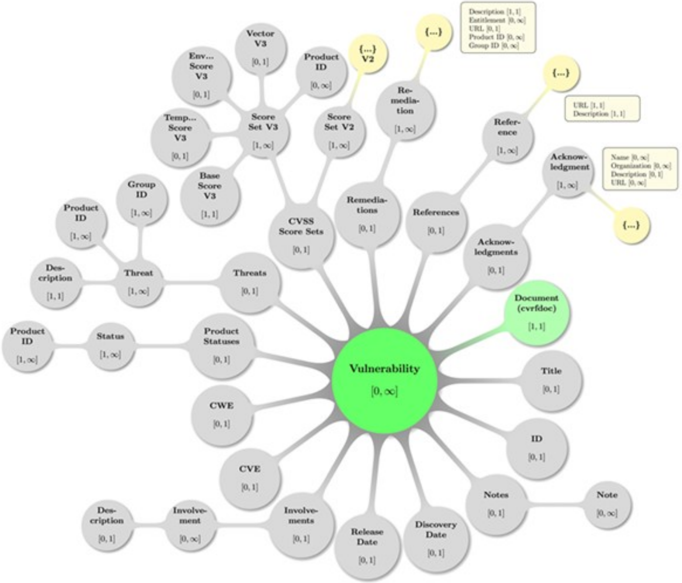
```
<CVE>CVE-2010-3864</CVE>
```



```
<Vulnerability xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/vuln">
    <CVE>CVE-2014-2721 password issue</CVE>
    <CVE>CVE-&lt;br /&gt;2014-2722 key issue</CVE>
    <CVE>CVE-&lt;br /&gt;2014-2723 permission issue</CVE>
</Vulnerability>
```



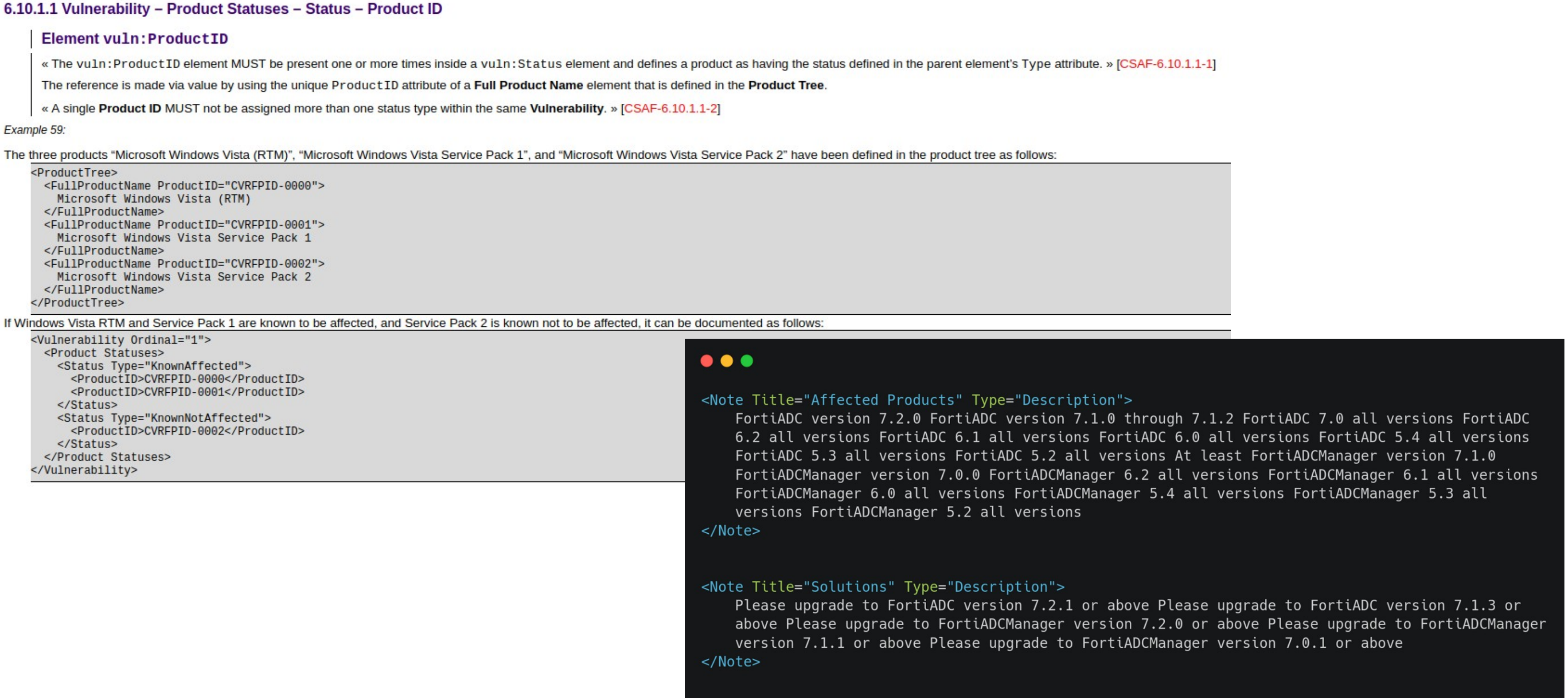
```
<Vulnerability xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/vuln">
    <CVE>CVE-2020-11896 to 2020-11914</CVE>
</Vulnerability>
```



[1] http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-14-010
[3] https://www.fortiguard.com/psirt/cvrf/FG-IR-20-104

# CVRF/CSAF の適したフィールドを利用しない

Product Tree を利用するのではなく、 Notes にすべて書いてしまっている



### 6.10.1.1 Vulnerability – Product Statuses – Status – Product ID

**Element `vuln:ProductID`**

« The `vuln:ProductID` element MUST be present one or more times inside a `vuln:Status` element and defines a product as having the status defined in the parent element's `Type` attribute. » [CSAF-6.10.1.1-1]

The reference is made via value by using the unique `ProductID` attribute of a **Full Product Name** element that is defined in the **Product Tree**.

« A single **Product ID** MUST not be assigned more than one status type within the same **Vulnerability**. » [CSAF-6.10.1.1-2]

*Example 59:*

The three products "Microsoft Windows Vista (RTM)", "Microsoft Windows Vista Service Pack 1", and "Microsoft Windows Vista Service Pack 2" have been defined in the product tree as follows:

```
<ProductTree>
  <FullProductName ProductID="CVRFPID-0000">
    Microsoft Windows Vista (RTM)
  </FullProductName>
  <FullProductName ProductID="CVRFPID-0001">
    Microsoft Windows Vista Service Pack 1
  </FullProductName>
  <FullProductName ProductID="CVRFPID-0002">
    Microsoft Windows Vista Service Pack 2
  </FullProductName>
</ProductTree>
```

If Windows Vista RTM and Service Pack 1 are known to be affected, and Service Pack 2 is known not to be affected, it can be documented as follows:

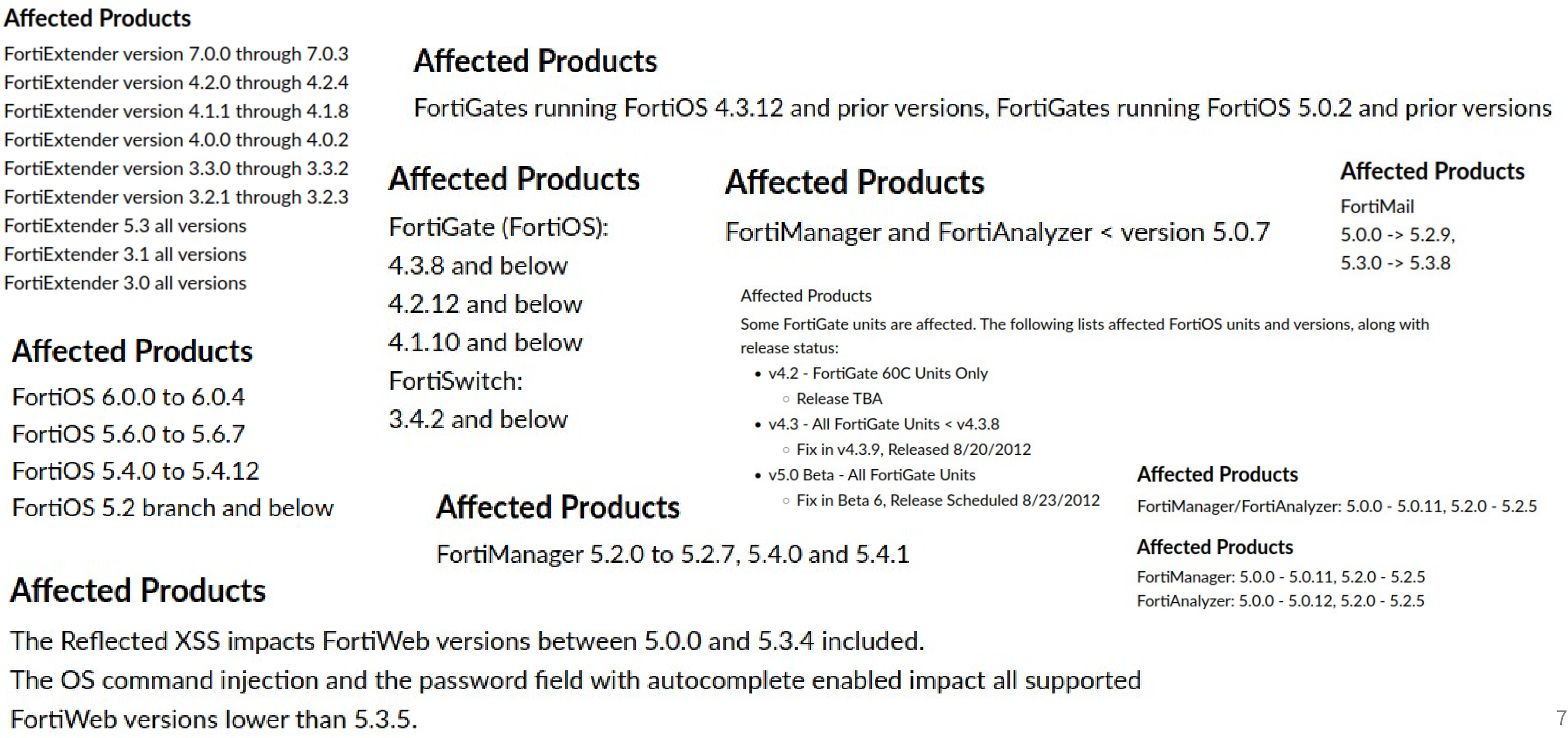
```
<Vulnerability Ordinal="1">
  <Product Statuses>
    <Status Type="KnownAffected">
      <ProductID>CVRFPID-0000</ProductID>
      <ProductID>CVRFPID-0001</ProductID>
    </Status>
    <Status Type="KnownNotAffected">
      <ProductID>CVRFPID-0002</ProductID>
    </Status>
  </Product Statuses>
</Vulnerability>
```

```
<Note Title="Affected Products" Type="Description">
    FortiADC version 7.2.0 FortiADC version 7.1.0 through 7.1.2 FortiADC 7.0 all versions FortiADC
    6.2 all versions FortiADC 6.1 all versions FortiADC 6.0 all versions FortiADC 5.4 all versions
    FortiADC 5.3 all versions FortiADC 5.2 all versions At least FortiADCManager version 7.1.0
    FortiADCManager version 7.0.0 FortiADCManager 6.2 all versions FortiADCManager 6.1 all versions
    FortiADCManager 6.0 all versions FortiADCManager 5.4 all versions FortiADCManager 5.3 all
    versions FortiADCManager 5.2 all versions
</Note>


<Note Title="Solutions" Type="Description">
    Please upgrade to FortiADC version 7.2.1 or above Please upgrade to FortiADC version 7.1.3 or
    above Please upgrade to FortiADCManager version 7.2.0 or above Please upgrade to FortiADCManager
    version 7.1.1 or above Please upgrade to FortiADCManager version 7.0.1 or above
</Note>
```

[1] http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-23-076

アドバイザリごとに異なるバージョン記述

機械的にプロダクトとバージョンの組み合わせを作ることが難しい



### Affected Products

FortiExtender version 7.0.0 through 7.0.3
FortiExtender version 4.2.0 through 4.2.4
FortiExtender version 4.1.1 through 4.1.8
FortiExtender version 4.0.0 through 4.0.2
FortiExtender version 3.3.0 through 3.3.2
FortiExtender version 3.2.1 through 3.2.3
FortiExtender 5.3 all versions
FortiExtender 3.1 all versions
FortiExtender 3.0 all versions

### Affected Products

FortiOS 6.0.0 to 6.0.4
FortiOS 5.6.0 to 5.6.7
FortiOS 5.4.0 to 5.4.12
FortiOS 5.2 branch and below

### Affected Products

FortiGates running FortiOS 4.3.12 and prior versions, FortiGates running FortiOS 5.0.2 and prior versions

### Affected Products

FortiGate (FortiOS):
4.3.8 and below
4.2.12 and below
4.1.10 and below
FortiSwitch:
3.4.2 and below

### Affected Products

FortiManager and FortiAnalyzer < version 5.0.7

### Affected Products

FortiMail
5.0.0 -> 5.2.9,
5.3.0 -> 5.3.8

Affected Products

Some FortiGate units are affected. The following lists affected FortiOS units and versions, along with release status:

- v4.2 - FortiGate 60C Units Only
  - Release TBA
- v4.3 - All FortiGate Units < v4.3.8
  - Fix in v4.3.9, Released 8/20/2012
- v5.0 Beta - All FortiGate Units
  - Fix in Beta 6, Release Scheduled 8/23/2012

### Affected Products

FortiManager/FortiAnalyzer: 5.0.0 - 5.0.11, 5.2.0 - 5.2.5

### Affected Products

FortiManager: 5.0.0 - 5.0.11, 5.2.0 - 5.2.5
FortiAnalyzer: 5.0.0 - 5.0.12, 5.2.0 - 5.2.5

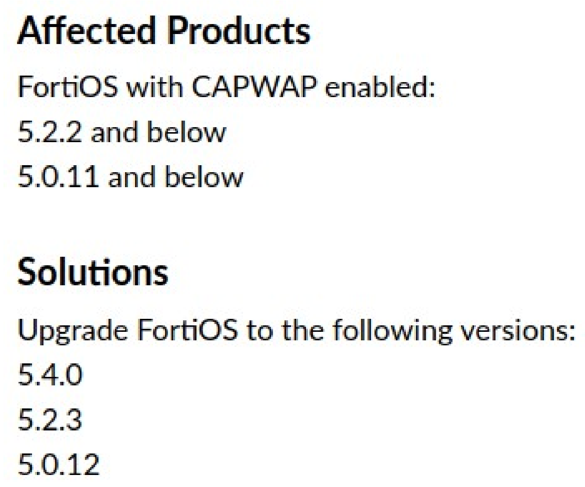
### Affected Products

FortiManager 5.2.0 to 5.2.7, 5.4.0 and 5.4.1

### Affected Products

The Reflected XSS impacts FortiWeb versions between 5.0.0 and 5.3.4 included.
The OS command injection and the password field with autocomplete enabled impact all supported FortiWeb versions lower than 5.3.5.

# 影響するバージョンはどこからどこまで？



**Affected Products**

FortiOS with CAPWAP enabled:

5.2.2 and below

5.0.11 and below

**Solutions**

Upgrade FortiOS to the following versions:

5.4.0

5.2.3

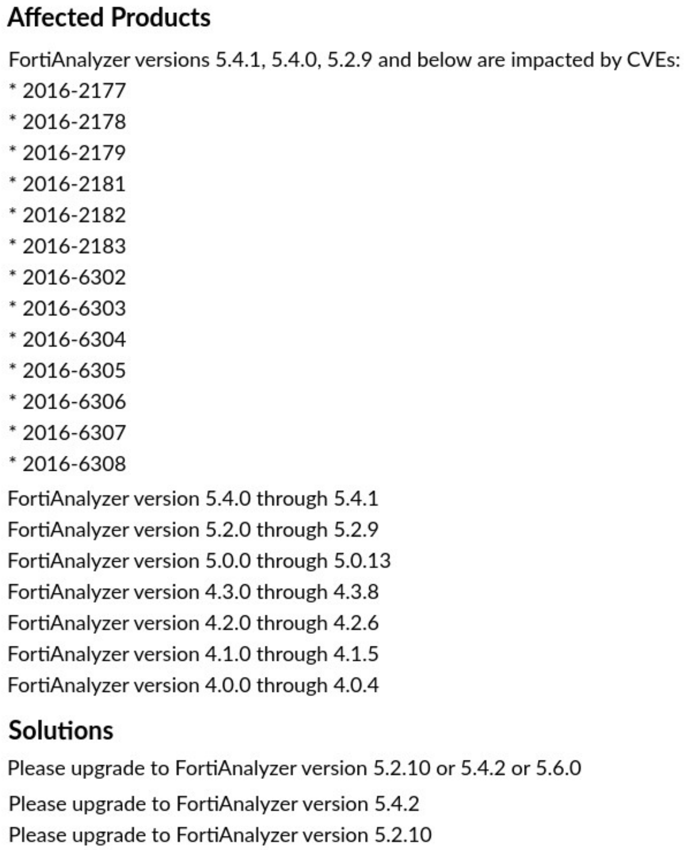
5.0.12

Affected Products から複数の解釈ができる
特に Solution を考慮しても、 2 と 3 を選べない

1. ≦ 5.0.11, ≦ 5.2.2
2. ≦ 5.0.11, ≧ 5.2.0, ≦ 5.2.2
3. ≧ 5.0.0, ≦ 5.0.11, ≧ 5.2.0, ≦ 5.2.2

https://www.fortiguard.com/psirt/FG-IR-15-002

# 同じプロダクトに対して、影響・修正バージョンが複数定義されている



**Affected Products**

FortiAnalyzer versions 5.4.1, 5.4.0, 5.2.9 and below are impacted by CVEs:

* 2016-2177
* 2016-2178
* 2016-2179
* 2016-2181
* 2016-2182
* 2016-2183
* 2016-6302
* 2016-6303
* 2016-6304
* 2016-6305
* 2016-6306
* 2016-6307
* 2016-6308

FortiAnalyzer version 5.4.0 through 5.4.1

FortiAnalyzer version 5.2.0 through 5.2.9

FortiAnalyzer version 5.0.0 through 5.0.13

FortiAnalyzer version 4.3.0 through 4.3.8

FortiAnalyzer version 4.2.0 through 4.2.6

FortiAnalyzer version 4.1.0 through 4.1.5

FortiAnalyzer version 4.0.0 through 4.0.4

**Solutions**

Please upgrade to FortiAnalyzer version 5.2.10 or 5.4.2 or 5.6.0

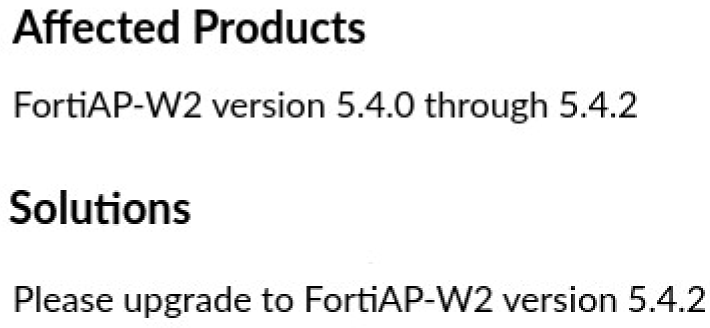
Please upgrade to FortiAnalyzer version 5.4.2

Please upgrade to FortiAnalyzer version 5.2.10

https://www.fortiguard.com/psirt/FG-IR-16-048

影響バージョンと修正バージョンで同じバージョンを指している

5.4.2 は affected or fixed ?



## Affected Products

FortiAP-W2 version 5.4.0 through 5.4.2

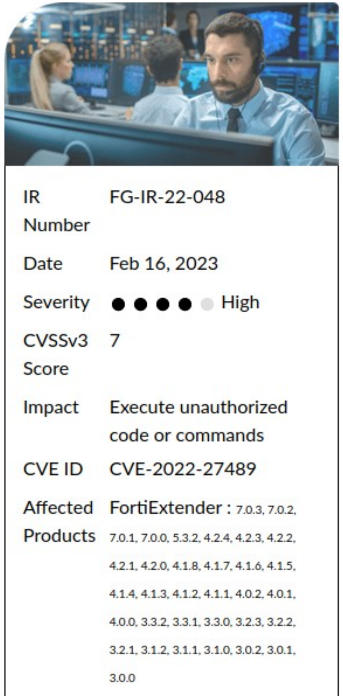
## Solutions

Please upgrade to FortiAP-W2 version 5.4.2

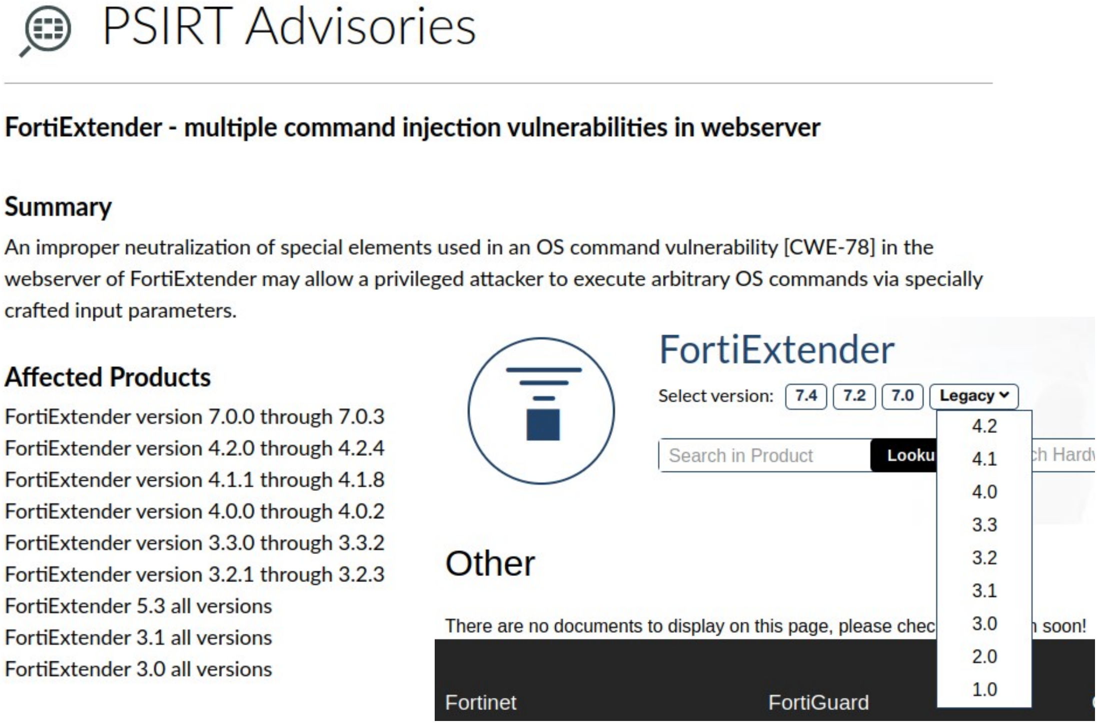
https://www.fortiguard.com/psirt/FG-IR-16-048

# 存在しないと思われるバージョンを参照している

FortiExtender 5.3 all versions と書いてあり、サイドバーには5.3.2が列挙されているが、ドキュメントでは5.3は存在しないようにみえる



| | |
|---|---|
| IR Number | FG-IR-22-048 |
| Date | Feb 16, 2023 |
| Severity | ● ● ● ● ○ High |
| CVSSv3 Score | 7 |
| Impact | Execute unauthorized code or commands |
| CVE ID | CVE-2022-27489 |
| Affected Products | FortiExtender : 7.0.3, 7.0.2, 7.0.1, 7.0.0, 5.3.2, 4.2.4, 4.2.3, 4.2.2, 4.2.1, 4.2.0, 4.1.8, 4.1.7, 4.1.6, 4.1.5, 4.1.4, 4.1.3, 4.1.2, 4.1.1, 4.0.2, 4.0.1, 4.0.0, 3.3.2, 3.3.1, 3.3.0, 3.2.3, 3.2.2, 3.2.1, 3.1.2, 3.1.1, 3.1.0, 3.0.2, 3.0.1, 3.0.0 |



## PSIRT Advisories

### FortiExtender - multiple command injection vulnerabilities in webserver

#### Summary

An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the webserver of FortiExtender may allow a privileged attacker to execute arbitrary OS commands via specially crafted input parameters.

#### Affected Products

FortiExtender version 7.0.0 through 7.0.3
FortiExtender version 4.2.0 through 4.2.4
FortiExtender version 4.1.1 through 4.1.8
FortiExtender version 4.0.0 through 4.0.2
FortiExtender version 3.3.0 through 3.3.2
FortiExtender version 3.2.1 through 3.2.3
FortiExtender 5.3 all versions
FortiExtender 3.1 all versions
FortiExtender 3.0 all versions

FortiExtender

Select version: 7.4 7.2 7.0 Legacy

Other

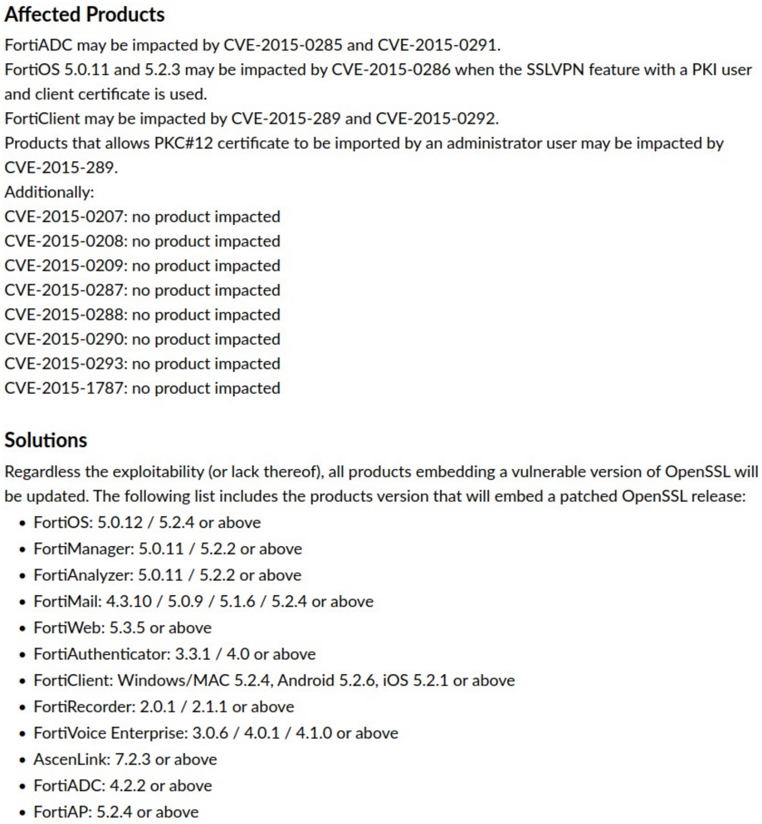
There are no documents to display on this page, please chec

soon!

[1] https://www.fortiguard.com/psirt/FG-IR-22-048 [2] https://docs.fortinet.com/product/fortiextender/5.3

# 対象となるプロダクトが具体的に書かれていない

> Products that allows PKC#12 certificate to be imported by an administrator user may be impacted by CVE-2015-289.



**Affected Products**

FortiADC may be impacted by CVE-2015-0285 and CVE-2015-0291.
FortiOS 5.0.11 and 5.2.3 may be impacted by CVE-2015-0286 when the SSLVPN feature with a PKI user and client certificate is used.
FortiClient may be impacted by CVE-2015-289 and CVE-2015-0292.
Products that allows PKC#12 certificate to be imported by an administrator user may be impacted by CVE-2015-289.
Additionally:
CVE-2015-0207: no product impacted
CVE-2015-0208: no product impacted
CVE-2015-0209: no product impacted
CVE-2015-0287: no product impacted
CVE-2015-0288: no product impacted
CVE-2015-0290: no product impacted
CVE-2015-0293: no product impacted
CVE-2015-1787: no product impacted

**Solutions**

Regardless the exploitability (or lack thereof), all products embedding a vulnerable version of OpenSSL will be updated. The following list includes the products version that will embed a patched OpenSSL release:

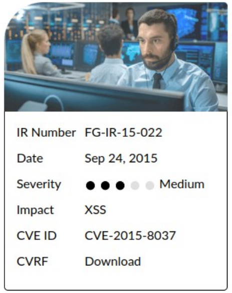
- FortiOS: 5.0.12 / 5.2.4 or above
- FortiManager: 5.0.11 / 5.2.2 or above
- FortiAnalyzer: 5.0.11 / 5.2.2 or above
- FortiMail: 4.3.10 / 5.0.9 / 5.1.6 / 5.2.4 or above
- FortiWeb: 5.3.5 or above
- FortiAuthenticator: 3.3.1 / 4.0 or above
- FortiClient: Windows/MAC 5.2.4, Android 5.2.6, iOS 5.2.1 or above
- FortiRecorder: 2.0.1 / 2.1.1 or above
- FortiVoice Enterprise: 3.0.6 / 4.0.1 / 4.1.0 or above
- AscenLink: 7.2.3 or above
- FortiADC: 4.2.2 or above
- FortiAP: 5.2.4 or above

https://www.fortiguard.com/psirt/FG-IR-15-008

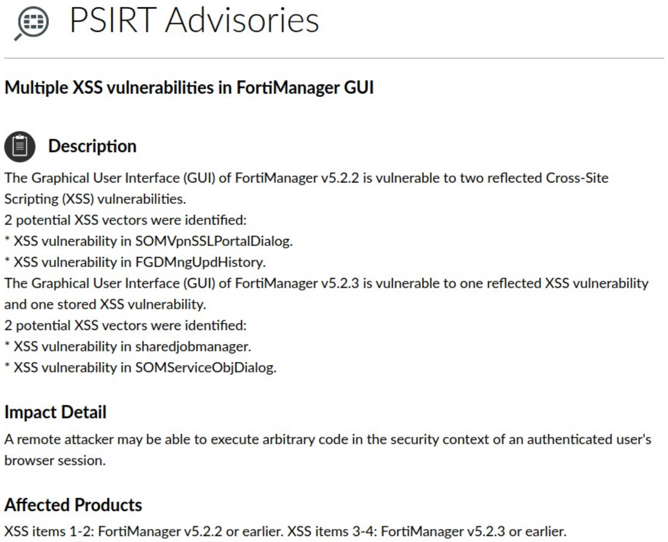
どの CVE を割り当てるべきか、公式アドバイザリだけでは完結しない

（e.g. アドバイザリに複数の CVE が紐づく場合、 CVRF を見る必要あり。

さらに、公式 Description と NVD を比較して、 item 1-2, item 3-4 へ CVE を割り当てる必要がある



| | |
|---|---|
| IR Number | FG-IR-15-022 |
| Date | Sep 24, 2015 |
| Severity | ●●●○○ Medium |
| Impact | XSS |
| CVE ID | CVE-2015-8037 |
| CVRF | Download |



PSIRT Advisories

**Multiple XSS vulnerabilities in FortiManager GUI**

**Description**

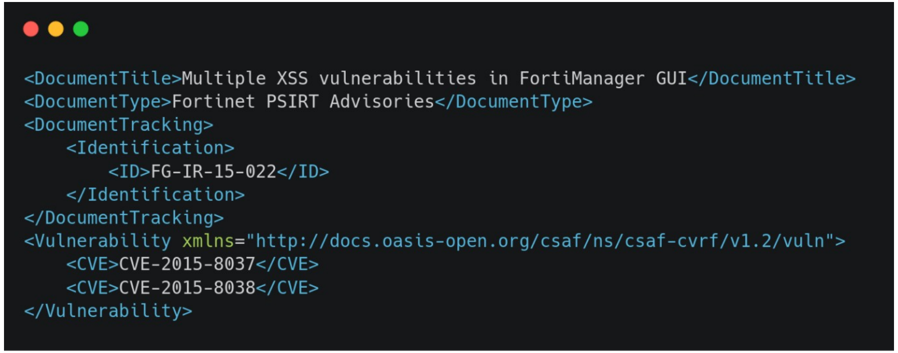
The Graphical User Interface (GUI) of FortiManager v5.2.2 is vulnerable to two reflected Cross-Site Scripting (XSS) vulnerabilities.
2 potential XSS vectors were identified:
* XSS vulnerability in SOMVpnSSLPortalDialog.
* XSS vulnerability in FGDMngUpdHistory.
The Graphical User Interface (GUI) of FortiManager v5.2.3 is vulnerable to one reflected XSS vulnerability and one stored XSS vulnerability.
2 potential XSS vectors were identified:
* XSS vulnerability in sharedjobmanager.
* XSS vulnerability in SOMServiceObjDialog.

**Impact Detail**

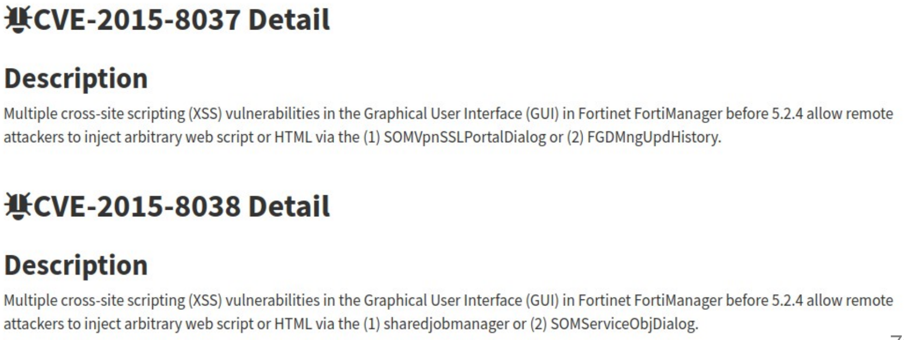
A remote attacker may be able to execute arbitrary code in the security context of an authenticated user's browser session.

**Affected Products**

XSS items 1-2: FortiManager v5.2.2 or earlier. XSS items 3-4: FortiManager v5.2.3 or earlier.



```
<DocumentTitle>Multiple XSS vulnerabilities in FortiManager GUI</DocumentTitle>
<DocumentType>Fortinet PSIRT Advisories</DocumentType>
<DocumentTracking>
    <Identification>
        <ID>FG-IR-15-022</ID>
    </Identification>
</DocumentTracking>
<Vulnerability xmlns="http://docs.oasis-open.org/csaf/ns/csaf-cvrf/v1.2/vuln">
    <CVE>CVE-2015-8037</CVE>
    <CVE>CVE-2015-8038</CVE>
</Vulnerability>
```



**CVE-2015-8037 Detail**

**Description**

Multiple cross-site scripting (XSS) vulnerabilities in the Graphical User Interface (GUI) in Fortinet FortiManager before 5.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) SOMVpnSSLPortalDialog or (2) FGDMngUpdHistory.

**CVE-2015-8038 Detail**

**Description**

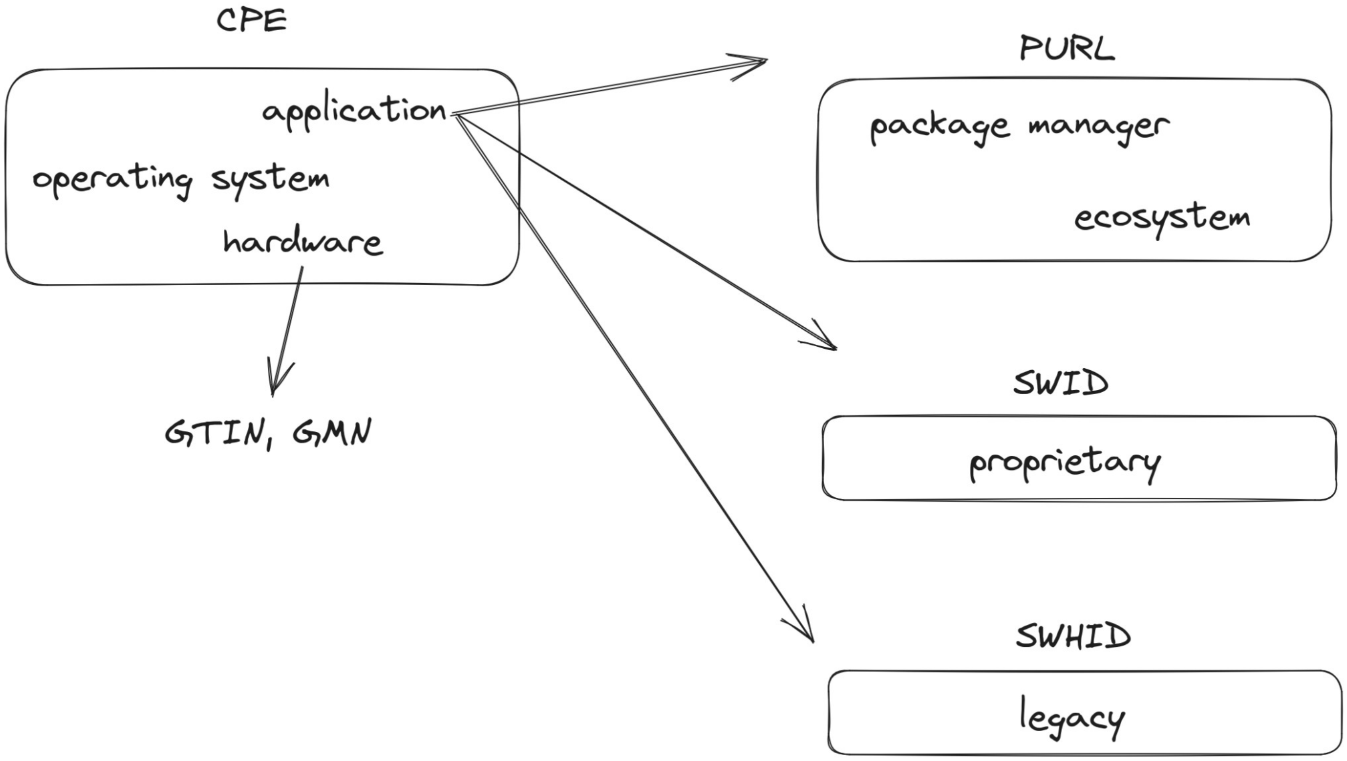
Multiple cross-site scripting (XSS) vulnerabilities in the Graphical User Interface (GUI) in Fortinet FortiManager before 5.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) sharedjobmanager or (2) SOMServiceObjDialog.

[1] https://www.fortiguard.com/psirt/FG-IR-15-022 [2] https://www.fortiguard.com/psirt/cvrf/FG-IR-15-022
[3] https://nvd.nist.gov/vuln/detail/CVE-2015-8037 [4] https://nvd.nist.gov/vuln/detail/CVE-2015-8038

# Appendix D:
# プロダクトの表現

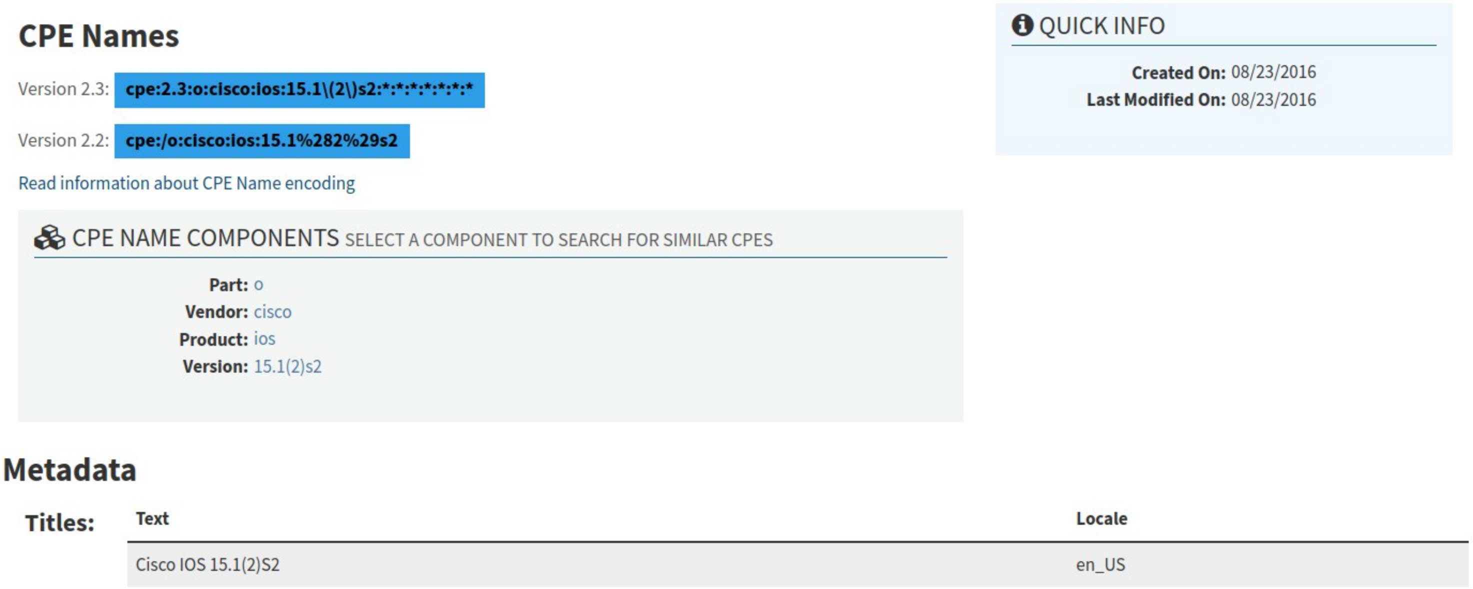
- CPE: Common Platform Enumeration
    - https://cpe.mitre.org/specification/
    - application, operating system, hardware や vendor, product, version などを表現できる
- PURL: Package URL
    - https://github.com/package-url/purl-spec
    - ソフトウェア向け
- SWID: Software ID
    - https://nvd.nist.gov/products/swid
    - PURL で表現できないようなパッケージマネージャを使わないプロプライエタリなソフトウェアを識別する
- SWHID: Software Heritage IDs
    - https://www.softwareheritage.org/
    - パッケージマネージャで利用できなくなったレガシーソフトウェアを識別する
- GTIN: Global Trade Identification Number
    - https://www.gs1.org/standards/id-keys/gtin
    - ハードウェア向け
- GMN: Global Model Number
    - https://www.gs1.org/standards/id-keys/global-model-number-gmn
    - 1 つの GMN に複数の GTIN を紐付けることができる

CPE は app や os、 hw を広く表現できるが、 naming problem などの課題が認識されている。
そのため、最近では CPE ではなく表現したいものにあった識別子を利用したいという流れがある



# CPE とは

CVSS （ BaseScore でよく使われている仕組み）で、ハードウェアやソフトウェアを識別するための共通の名称基準のこと。



## CPE Names

Version 2.3: cpe:2.3:o:cisco:ios:15.1\(2\)s2:*:*:*:*:*:*:*

Version 2.2: cpe:/o:cisco:ios:15.1%282%29s2

Read information about CPE Name encoding

CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

**Part:** o
**Vendor:** cisco
**Product:** ios
**Version:** 15.1(2)s2

QUICK INFO

**Created On:** 08/23/2016
**Last Modified On:** 08/23/2016

## Metadata

**Titles:**

| Text | Locale |
|---|---|
| Cisco IOS 15.1(2)S2 | en_US |

https://nvd.nist.gov/products/cpe/detail/4EA94F50-E948-4122-9927-3D2B4248755F?namingFormat=2.3&orderBy=CPEURI&keyword=cpe%3A2.3%3Ao%3Acisco%3Aios%3A15.1%5C%282%5C%29s2%3A&status=FINAL%2CDEPRECATED

# Appendix E:
# 脆弱性情報とプロダクトの紐付け

- OVAL
  - https://oval.mitre.org/
  - レンジ、 OS on HW が表現できる
- CVRF/CSAF
  - http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html
  - http://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
  - Product Tree で列挙する形のためレンジの表現が難しいが、 OS on HW を表現できる
- VEX
  - https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf
  - OS on HW, Version を ID にしてそれを参照する形？
- MITRE CVE
  - https://cveproject.github.io/cve-schema/schema/v5.0/docs/
  - レンジ (lt, le のみ ) が表現できる、 OS on HW は表現できない？
- NVD
  - https://csrc.nist.gov/schema/nvd/feed/1.1/nvd_cve_feed_json_1.1.schema
  - レンジ、 OS on HW が表現できる
  - 脆弱性情報とプロダクトの紐付けに CPE を利用している
- OSV
  - https://ossf.github.io/osv-schema/
  - レンジは表現できるが、 OS on HW は難しそう？