Cisco Security Advisory
24 January 2007

Miya Kohno @ janog19 PC

最初に

- よりによってこんなときに。
- ご迷惑をおかけした皆様、大変申し訳ありません。

Agenda

- 3つのSA
- 情報

3つのSA

1. Crafted IP Option
2. Crafted TCP packet
3. Crafted IPv6 packet header

Crafted IP Option

1. 概要

偽造されたIP optionを持つパケットを受信した際にRouterが異常処理/crashする可能性があります。
異常処理の原因となりうるProtocolは、**ICMP, PIMv2, PGM, URD**。

- 他のプロトコル、IPv6 packetは、本SAの該当ではありません。
- 通過パケットはトリガになりません。

2. 対象OS

IOS : 9.x, 10.x, 11.x and 12.x
IOS-XR : 2.0.X, 3.0.X, and 3.2.X

3. Workaround

1. IP Options Selective Drop
   但し、正しいIP optionsもdropしてしまう可能性があるため、次のようなProtocolを使用している場合は適用不可。RSVP, MPLS TE, MPLS OAM, DVMRP, IGMPv3, IGMPv2, PGM
2. Infra ACL, rACL
3. CoPP

Crafted TCP packets

1. 概要

偽造された、該当ルータへの**TCP パケット**が、メモリーリークの原因になる可能性があります。(**IOS** TCP listner の脆弱性)

- IPv6 packet、IOS-XR は、本SA の該当ではありません。
- 通過パケットはトリガになりません。

2. 対象OS

全てのIOS (9.x, 10.x, 11.x and 12.x)

3. Workaround

1. Infra ACL, rACL
2. CoPP
3. uRPF
4. BGP 用にBTSH/GTSM

Crafted IPv6 Header

1. 概要

偽造された**IPv6 Type0 Routing Header**（IPv6 source routingに使用される）を受けると、**IOS**がCrashする可能性があります。（IPv6が設定されている場合、Source Routingはdefaultでenableになっています。）

- IPv6 type2 Routing Header、IOS-XRは、本SAの該当ではありません。
- 通過するパケットはトリガになりません。

2. 該当IOS

IPv6がenableされたIOS

Crafted IPv6 Header (続き)

3. Workaround

1) Mobile IPを使用していない場合

- 12.3(4)T より前 : ACLsにより、Routing header(0,2)を含むパケットをdropする。
- 12.3(4)T以降 ：ipv6 source-route コマンドにより、Routing header(0,2)を含むIPv6パケットをblockする。

2) Mobile IPを使用している場合

- 12.4(2)T より前 : ワークアラウンドなし
- 12.4(2)T以降: IPv6 ACLsにてrouting-typeを指定

情報

情報を充分吟味し、必要なワークアラウンドを講じてください。

- http://www.cisco.com/go/psirt
- 日本語訳 (*)
  - IP Opction
    http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-crafted-ip-option-j.shtml
  - TCP packets
    http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-crafted-tcp-j.shtml
  - IPv6 routing header
    http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-IOS-IPv6-j.shtml
  - 今回の3つの脆弱性全てに対処するIOSの表:
    http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-bundle-j.shtml

(*) 基情報と食い違いがある場合は、基情報を優先します。

n

- CVSS score

CVSS

- **CVSS : Common Vulnerability Scoring System**
  FIRSTの呼びかけによる、脆弱性に関する深刻度評価の標準化
  http://itpro.nikkeibp.co.jp/article/USNEWS/20050921/221466/

- Cisco WEB Q&A
  http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

- Cisco WEB CVSS calculator
  https://intellishield.cisco.com/security/alertmanager/cvss