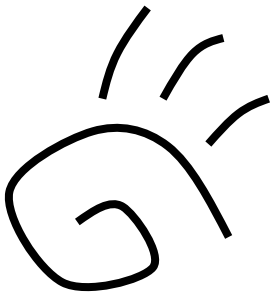


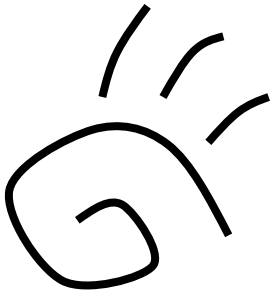
ぼくの考えたさいきょうのDevSecOps

2017/1/19

Vulsといかれたメンバー

「セキュリティは経営課題！」

- 脆弱性が出ると「すぐにパッチを当てろ」とのお達しが
  - × 今年はBINDが当たり年！（いや、困るよ……）
- どこまで影響出るんだよ……時間かかるよ……　ざわ……ざわ……
- 「その間どうやって守るんだよ！？」とか言われても……



NW機器も脆弱性が！

» 脆弱性はサーバだけじゃない！

» ルータやFW, UTMなど外側のNW機器にも！

[redacted]に情報漏洩の脆弱性 - 「Shadow Brokers」のエクスプロイト調査中に判明

[redacted]のネットワーク機器向けソフトウェア[redacted]「同XE」「同XR」に、情報漏洩の脆弱性が存在することが明らかとなった。同社はアップデートの準備を進めている。

これらソフトウェアの一部バージョンに、「IKEv1」のパケット処理においてメモリの内容が取得される脆弱性「CVE-2016-6415」が存在することが判明したもの。リモートより認証なく攻撃が可能で、重要度は、4段階中上から2番目にあたる「高（high）」にレーティングされている。

影響を受けるソフトウェアを搭載した機器において、「IKEv1」のネゴシエーションを受け入れる設定の場合、細工したパケットを利用して、機密情報を取得されるおそれがある。

ZDNet Japan

編集部からのお知らせ
• 海外ニュース記事ライター（フリーランス）募集

CIO | クラウド | モバイル PC | セキュリティ | ソフトウェア | サーバ | ストレージ | ネットワーク | ミドルウェア | 運用 | マーケティング

ZDNet Japan > セキュリティ

脆弱性が発見された[redacted]の「[redacted]」にデフォルトのバックドアパスワード

Chris Duckett （ZDNet.com） 翻訳校正： 編集部 2015年12月22日 11時02分

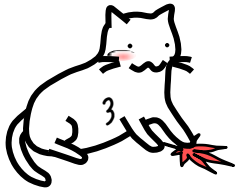
Tweet B!

印刷 | メール | ダウンロード | クリップ

先週脆弱性が判明した[redacted]nOS」にデフォルトのパスワードが存在することを、セキュリティ企業Rapid7が明らかにした。

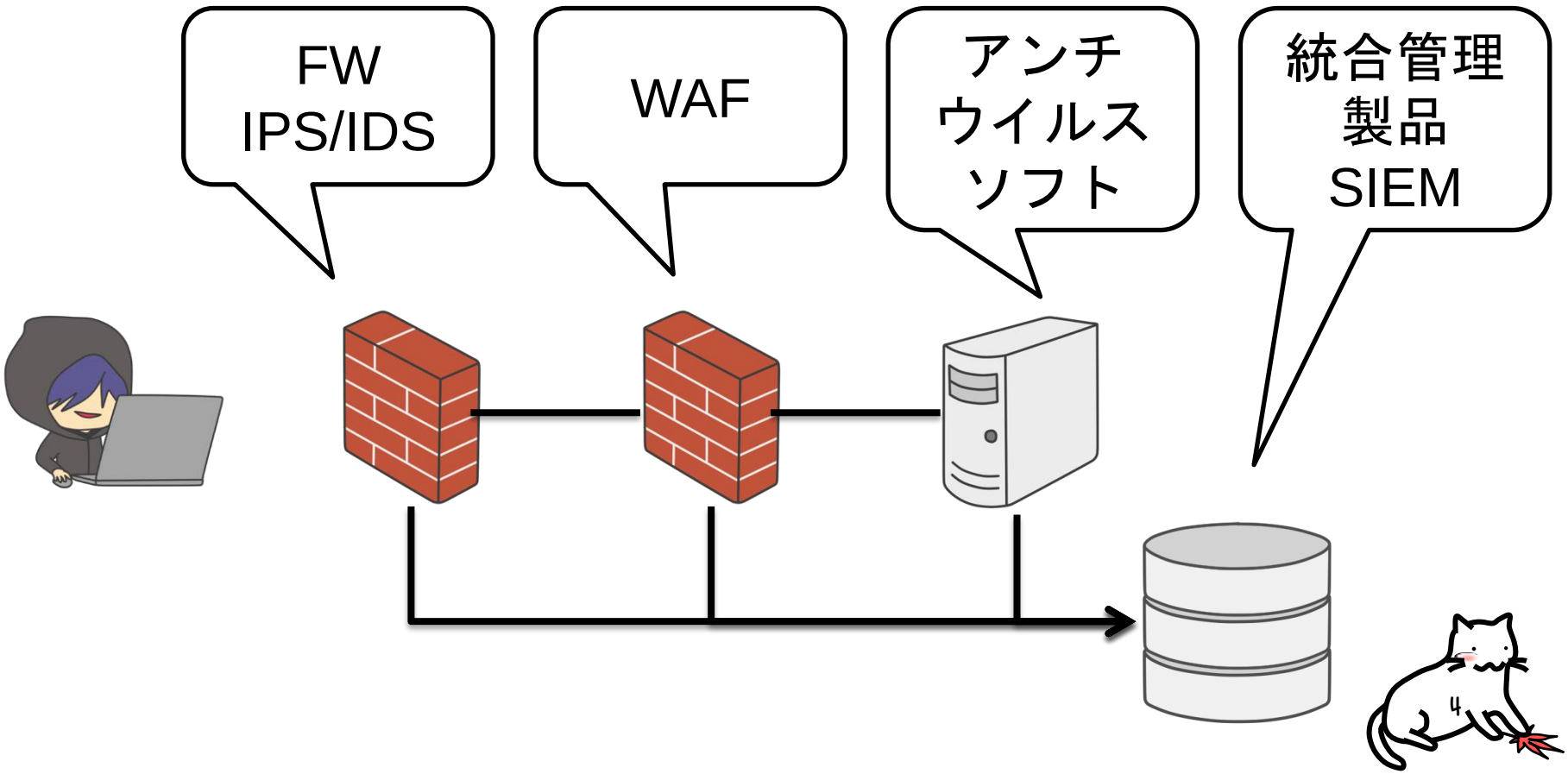
Rapid7の最高セキュリティ責任者、HD Moore氏はブログで[redacted]のパッチが当てられたバージョンと脆弱なバージョンとの違いをstrcmp呼び出しにフォーカスして調べていて、パスワードの存在に気付いたという。パスワードは<<< %s(un='%s') = %uだ。これを知っていれば、有効なユーザー名があればログインが可能になるという。

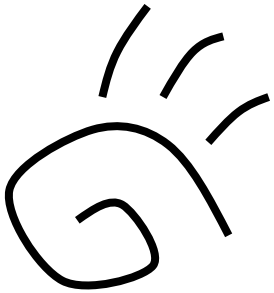
[redacted]は先週、内部のコードレビューにより[redacted]に2件の脆弱性を発見したことを報告した。1つ目は攻撃者が足跡を残さずにVPNトラフィックを復号するこ



お金の力で！

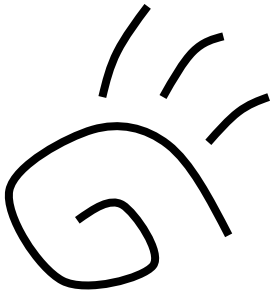
» お金で緩和する方法もとれるかも？





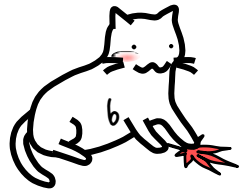
え！

本当に！？



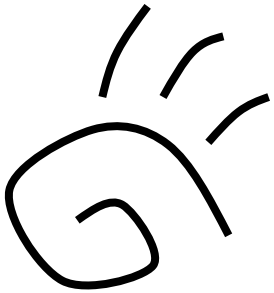
じゃあどうしよう？

- 放置はできない…
- 本来はちゃんとパッチを当てて適切に設定できているかどうか、のはず
- 0円でOSSで自動でリリース判定までできて可視化できたらいいなあ



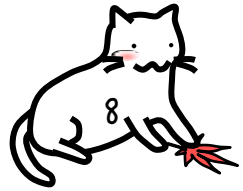
議論したいDevSecOpsとは

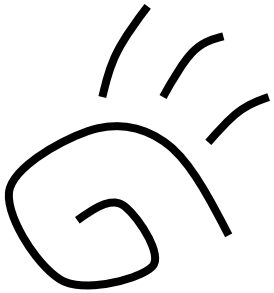
- 脆弱性が出たらパッチを適用
- 全レイヤーでの試験を実施し、リリース判断
- 関係者全員が一目瞭然で状況が見える
- そんなこといいな、できたらいいな



組み合わせてみよう！OSSで！

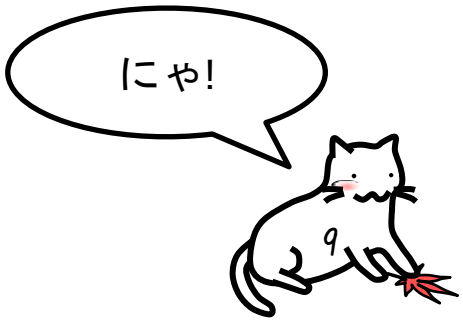
壮大な夢





まてまてーい！

Vulsだよ！



議論したい！

- みなさん、どうしてますか？
- これって使えそうだと思いましたか？
- どんなツールで運用を実践してますか？
- 他にいいツールを知りませんか？

今週の中吊り大賞

巻頭スクープ！
まだ脆弱性で消耗しているの？

海外を目指す破壊の言葉。その先には

袋とじ特別企画
momoさんちの猫

師走を賑わす街の話題

ハワイで直撃！ヒューチャーさんマジヒューチャー！

サウナで健康に！必勝入浴法

「せんべろ」ならこのお店

[連載]yujiおすすめ「今日はこのお店」

実録！●●ソフトのなくなる日
「こんな会社潰れちゃえ、って思ってました」

コンビニ駅の売店にない

週刊罵流洲