

脆弱性スキャナによる対策支援の課題

フューチャーアーキテクト株式会社
Technology Innovation Group
神戸 康多

自己紹介

- 神戸康多（かんべこうた）
- フューチャーアーキテクト株式会社所属
- サウナが趣味（週2）
- Linux/FreeBSD向け脆弱性スキャナVuls作者 [GitHub](#)

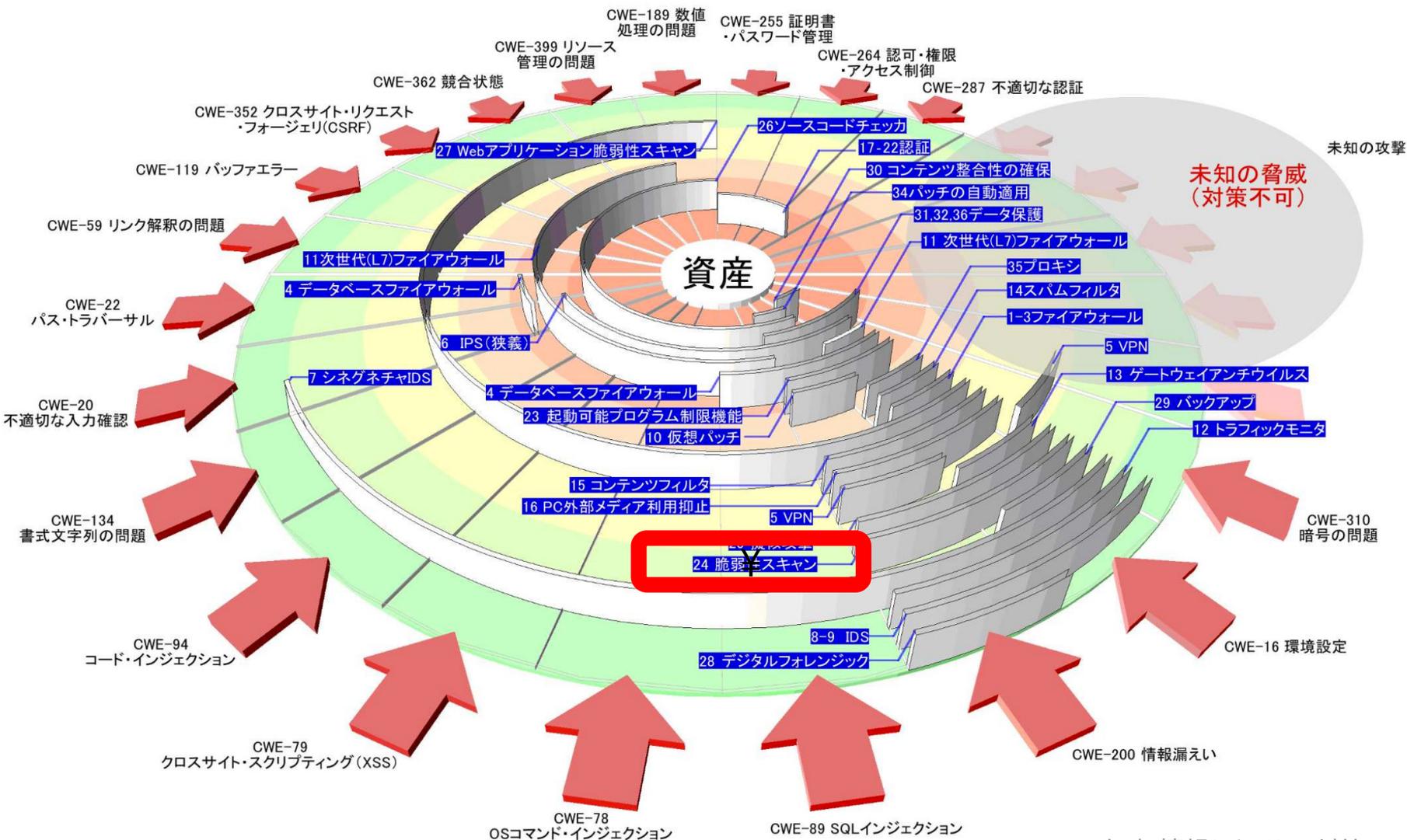


本日のテーマ

- I. IPS/IDS/Antivirusではカバーできない脆弱性を紹介。
Linuxサーバでのパッケージ、ライブラリなどのアップデートの重要性を知る。
- II. 人力での脆弱性対策の大変さを知る。
- III. OSSの脆弱性スキャナVulsを用いて、**楽に、漏れなく、無料で**出来る脆弱性対策の一例を紹介する。

本日の対象範囲

Linuxシステムの、24. 脆弱性スキャンが対象



JNSA 2013年度 情報セキュリティ対策マップより

IDS/IPS, Antivirusでは防げない脆弱性も存在する

- Dirty Cow (CVE-2016-5195)
- SSH接続可能な一般ユーザがRootへ権限昇格可能な脆弱性
- 内部犯行可能
 - ✓ 運用ルールで一般ユーザ、Rootユーザを分けていても、数秒で一般ユーザがRootユーザに権限昇格可能
- SSHで接続可能なユーザであれば誰でも簡単に実行可能
 - ✓ PoCが沢山公開されている
 - ✓ <https://dirtycow.ninja/>
- PoCをカスタマイズすればIDS/IPS, Antivirusでの検知は難しい

Linuxサーバもソフトウェアアップデートは必要

OSパッケージ、ライブラリアップデート方法は2種類

- プロダクション環境は**手動アップデート**を採用するケースが多い

自動アップデート

メリット

- 手間なし
- 漏れなし

デメリット

- **サービスダウン**の可能性
 - ✓ ミドルウェア、ライブラリのAPIが変更される可能性

手動アップデート

メリット

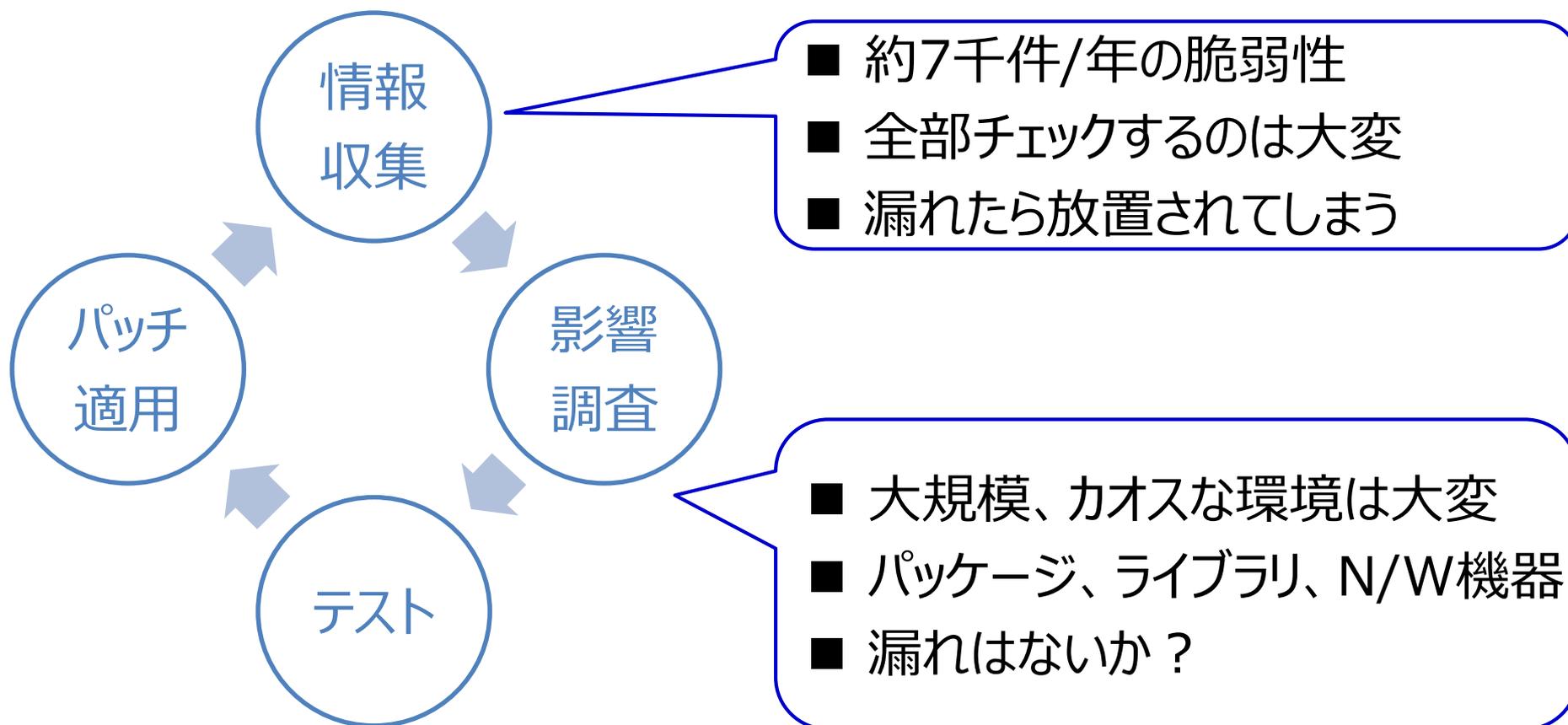
- 事前に**テスト可能**

デメリット

- 脆弱性情収集、影響調査の**コスト大**
- **漏れる**可能性あり

手動アップデート運用での脆弱性対策は大変

- 日々公開される脆弱性情報を追い続ける必要がある
- システム運用者は以下のサイクルを日々回している



毎日の大変な作業は自動化すべき

Vulsは脆弱性情報の収集、影響度調査を自動化する

- 日々の情報収集、影響度調査を自動化
- パッチ適用漏れによる脆弱性の放置を防ぐ



私が作りました

Vulsを作った経緯

100台規模のLinux環境を運用した経験より…

- Ubuntu, CentOS, Debianなどディストリビューション、バージョンもバラバラ。Ruby, Javaなど複数の言語

人力での脆弱性対策が大変だった

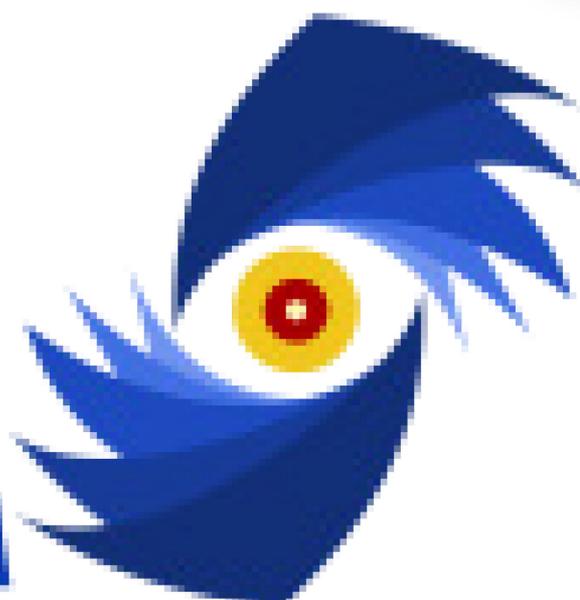
- 日々公開される脆弱性情報を全てチェック
- 影響調査
- 見逃してないか？ 調査結果は正しいか？
- またOpenSSLか…



Vulsは怒りと憎しみから生まれた

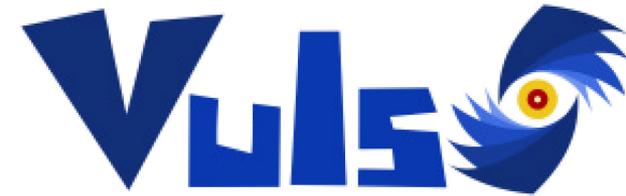
Fork me on GitHub

VLS



Vuls概要

- 潜在する脆弱性と該当サーバを可視化
- 定期実行で対策漏れがなくなる



Vulsの特徴

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 世界で注目のOSS

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

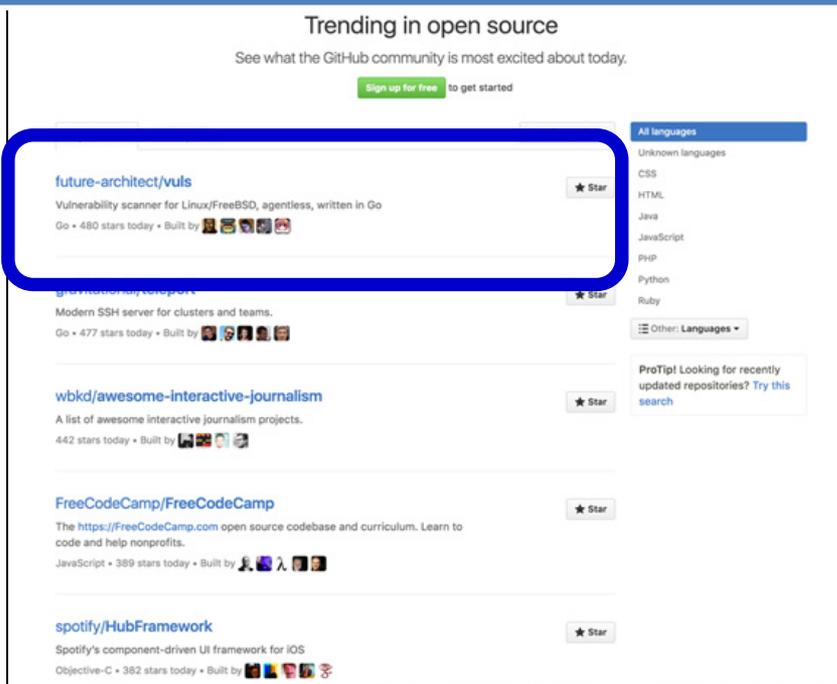
Vulsの特徴 世界で注目のOSS

■ 2016/4/1 GitHub公開

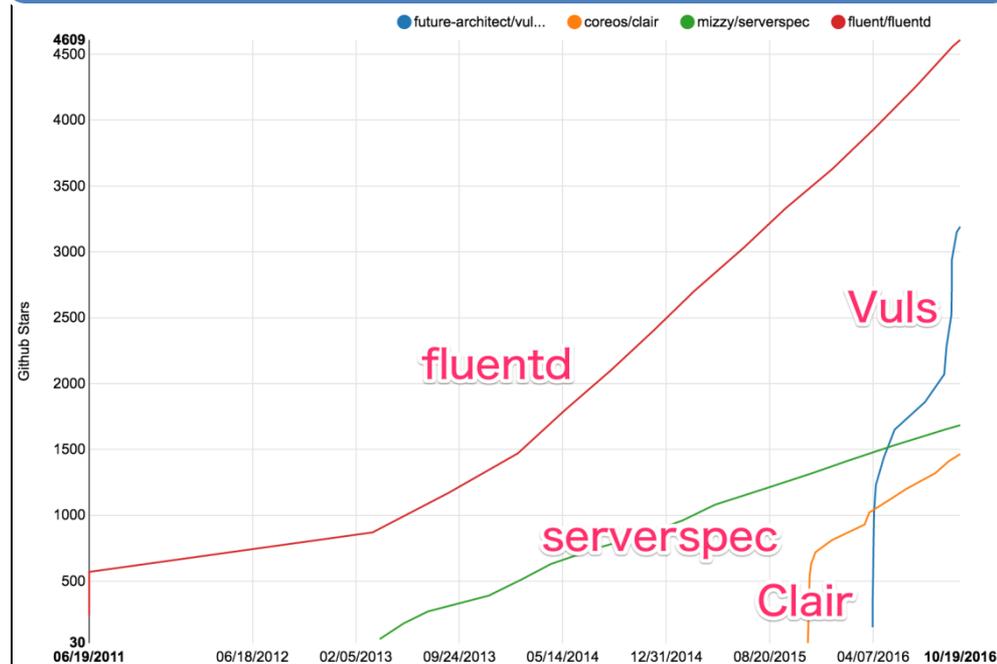
✓ <https://github.com/future-architect/vuls>

■ 公開直後から世界中で話題になり、2016/10/1にGitHubスター獲得ランキング全言語1位に

世界1位



スター数は順調に増加



Vulsの特徴 エージェントレス

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 エージェントレス

セットアップが簡単

- 1台のみでよい

既に動いている本番環境に導入しやすい

- 既存本番環境にエージェントを入れたくない/入れられないケースでも導入可能

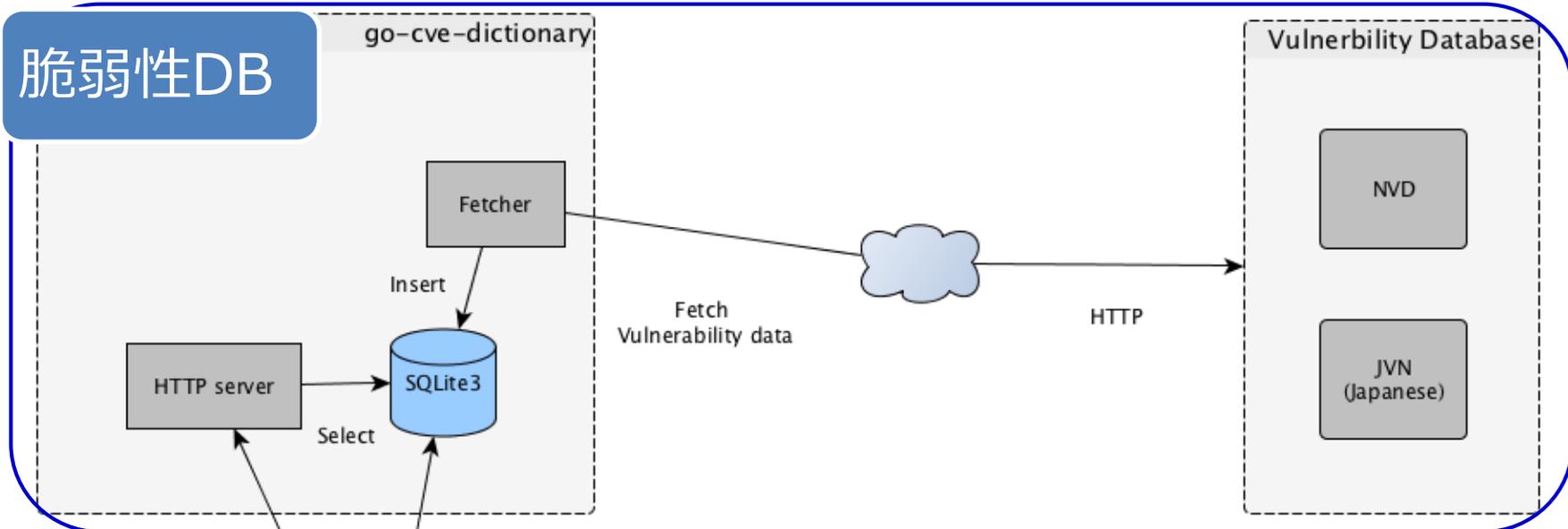
大規模環境向き

- Vuls本体のデプロイ、アップデートが簡単

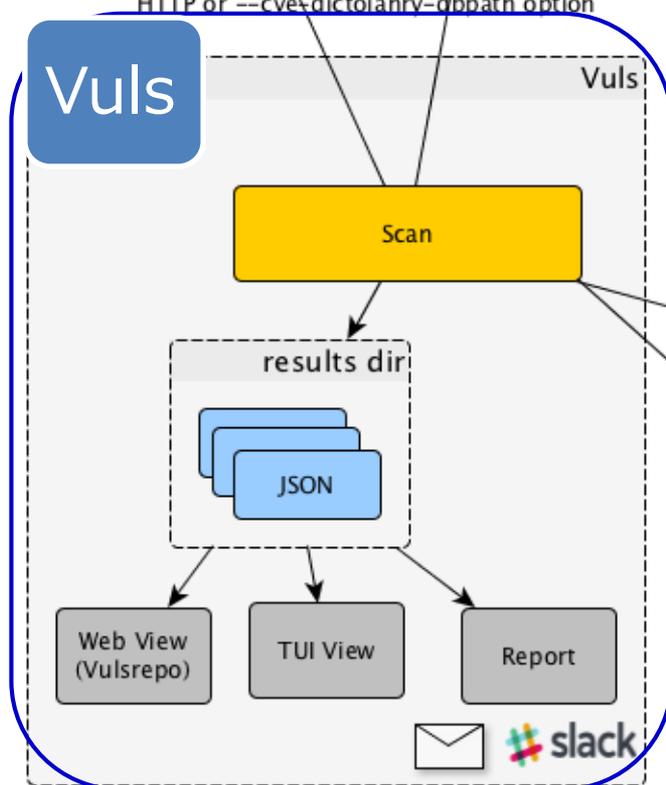
Vulsサーバから対象サーバにはSSHで接続

- 対象サーバ上でコマンドを発行（ホワイトボックス）
- 非破壊テスト型スキャナ

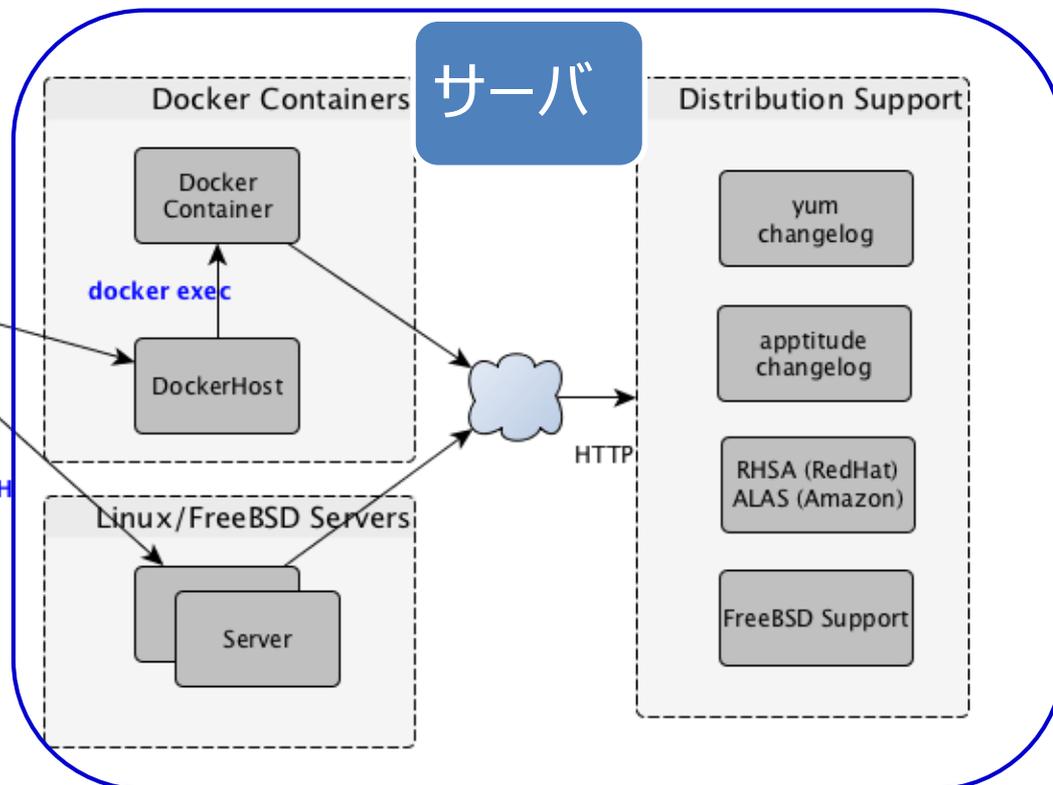
脆弱性DB



Vuls



サーバ



Vulsの特徴 日本語レポート

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 日本語レポート

■ Slack, E-mail通知に対応 (2016/11時点)

The screenshot shows a Slack interface for the channel #centos20052. The left sidebar lists channels and direct messages. The main area displays four vulnerability notifications, each with a title, severity, description, and a table of installed vs. candidate packages.

CVE ID	Severity	Description	Installed	Candidate
CVE-2015-7181	7.5 (High)	Mozilla Firefox などの製品で使用される Network Security Services におけるサービス運用妨害 (DoS) の脆弱性	nss-3.16.2.3-1.el5_11	nss-3.19.1-4.el5_11
CVE-2015-8704	6.8 (Medium)	ISC BIND の apl_42.c におけるサービス運用妨害 (DoS) の脆弱性	bind-libs-9.3.6-25.P1.el5_11.2 bind-utils-9.3.6-25.P1.el5_11.2	bind-libs-30:9.3.6-25.P1.el5_11.8 bind-utils-30:9.3.6-25.P1.el5_11.8
CVE-2013-7424	5.1 (Medium)	GNU C Library の getaddrinfo 関数におけるサービス運用妨害 (DoS) の脆弱性	glibc-2.5-123.el5_11.1 glibc-common-2.5-123.el5_11.1	glibc-2.5-123.el5_11.3 glibc-common-2.5-123.el5_11.3
CVE-2015-0286				

Vulsの特徴 OSパッケージ、言語ライブラリ、N/W機器に対応

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 OSパッケージ、言語ライブラリ、N/W機器に対応

- CPE登録済みのものであれば脆弱性の検知が可能
- 参考: IPA共通プラットフォーム一覧CPE概説
 - ✓ <https://www.ipa.go.jp/security/vuln/CPE.html>

Vulsの設定ファイル RoR4.2.1を定義した例

```
[servers]

[servers.172-31-4-82]
host      = "172.31.4.82"
user      = "ec2-user"
keyPath   = "/home/username/.ssh/id_rsa"
cpeNames = [
  "cpe:/a:rubyonrails:ruby_on_rails:4.2.1",
]
```

CPEの調べ方その1

- NVDで検索する
- <https://web.nvd.nist.gov/view/cpe/search>

CPEの調べ方その2

- NVDでの検索は面倒という方のためのツール
- ターミナルでインクリメンタル検索可能
- <https://github.com/kotakanbe/go-cpe-dictionary>

それでも面倒という方は…

Vulsの特徴 OSパッケージ、ライブラリ、N/W機器にも対応

- プログラミング言語ライブラリ用脆弱性スキャナ OWASP Dependency-Checkと連携する方法
- 利点
 - ✓ Vulsの設定ファイルにライブラリのCPEを定義しなくてよい
 - ✓ バージョンアップ時にVuls設定ファイルの変更不要
 - ✓ Vulsと連携すると日本語でのレポートが可能

Vulsの設定ファイル

```
[servers]
[servers.172-31-4-82]
host      = "172.31.4.82"
user      = "ec2-user"
keyPath   = "/home/username/.ssh/id_rsa"
dependencyCheckXMLPath = "/tmp/report.xml"
```

Vulsの特徴 対象OSが幅広い

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 対象OSが幅広い

- Linux系OS, FreeBSDの脆弱性をスキャン可能
- サポート期間中のものが対象

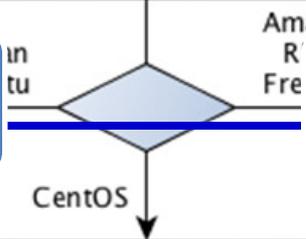
Redhat系	RHEL	(5), 6, 7 ※ RHEL5は対応予定
	CentOS	5, 6, 7
	Amazon Linux	全バージョン
Debian系	Debian	7, 8
	Ubuntu	12, 14, 16
BSD	FreeBSD	10, 11

OSごとのスキャンフロー

Get installed packages
Debian/Ubuntu: dpkg-query
Amazon/RHEL/CentOS: rpm
FreeBSD: pkg

Debian/Ubuntu/CentOS

RHEL/Amazon/FreeBSD



Check upgradable packages
Debian/Ubuntu: apt-get upgrade --dry-run

Get all changelogs of updatable packages at once
CentOS: yum update --changelog

Get CVE IDs by using package manager
Amazon/RHEL: yum plugin security
FreeBSD: pkg audit

foreach
upgradable packages

Parse changelogs and get CVE IDs

Parse changelog and get CVE IDs
Debian/Ubuntu: aptitude changelog

end loop

未アップデート部分の
チェンジログを解析

コマンドで取得

Vulsの特徴 対象OSが幅広い - チェンジログ解析の理由

- 脆弱性情報には該当するパッケージ、バージョン情報が含まれる。実装前はバージョンの比較で実現できるだろうと思っていたが、以下の通りバージョン比較での実現は不可能であることを悟る

Ubuntuパッケージ、バージョンの例

locales	2.13+git20120306-21
login	1:4.1.5.1-1.1ubuntu7
lsb-base	9.20160110
make	4.1-6
mawk	1.3.3-17ubuntu2
mime-support	3.59ubuntu1
multiarch-support	2.21-0ubuntu5

試行錯誤の末、チェンジログの解析を思いつく

Vulsの特徴 プラットフォーム非依存

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

プラットフォーム非依存

WebUI

Vulsの特徴 プラットフォーム非依存

オンプレ、クラウドどこでも動作

- SSH接続できればスキャン可能
- Vuls本体はGo言語製のプログラム

Dockerコンテナの脆弱性もスキャン可能

- DockerホストにSSH接続
コンテナへはdocker execでコマンド発行
- DockerコンテナにはSSHデーモンを起動しなくてもよい

Vulsの特徴 WebUI

世界で注目のOSS

エージェントレス

日本語レポート

OSパッケージ、言語ライブラリ、N/W機器に対応

対象OSが幅広い

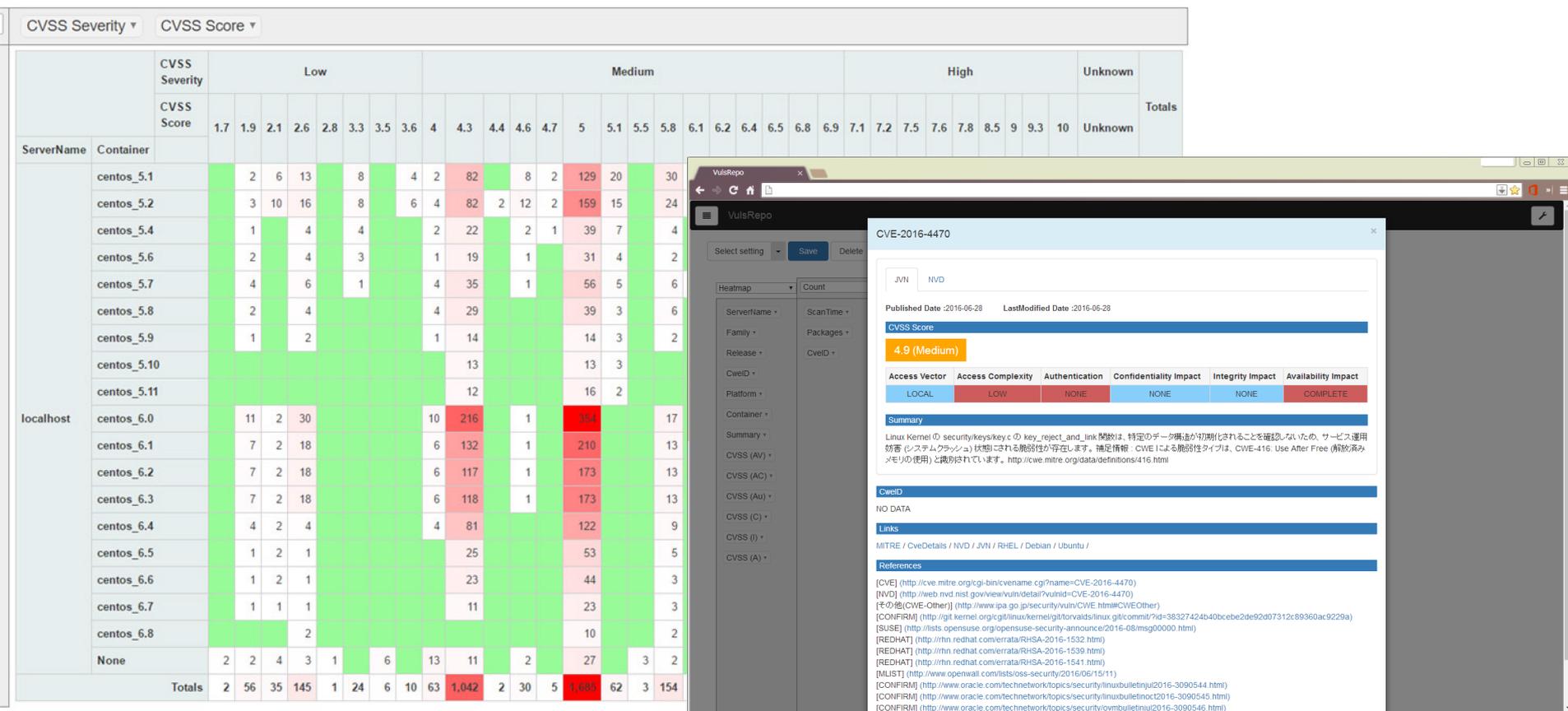
プラットフォーム非依存

WebUI

Vulsの特徴 WebUI

VulsRepo

- Excelのピボットテーブルのようにスキャン結果の分析が可能
- <https://github.com/usiusi360/vulsrepo>



Vulsの特徴 WebUI

Faraday

- 現在、Vulsプラグイン作成中
- <https://github.com/infobyte/faraday>

FARADAY

Dashboard for demo_faraday (all vulns) Change workspace View confirmed vulns

Top Services **Top Hosts** **Vulnerabilities**

Services report

18	18	9	5
WWW	SSH	UNKNOWN	HTTP
4	3	3	3
TELNET	FTP	RPCBIND	PRINTER?

Workspace summarized report

42	30	111	47	120
HOSTS	NOTES	SERVICES	WEB VULNS	VULNS
167				
TOTAL VULNS				

Last Vulnerabilities

Date	Target	Severity	Name	Web	Ease of resolution
11/11/2015 at 4:04PM	192.168.20.23	med	Service Detection	✗	
11/11/2015 at 4:04PM	192.168.20.23	med	Skype Stack Version Detection	✗	
11/11/2015 at 4:04PM	192.168.20.10	med	SNMP Protocol Version Detection	✗	
11/11/2015 at 4:04PM	192.168.20.10	med	TCP/IP Timestamps Supported	✗	
11/11/2015 at 4:04PM	192.168.20.10	med	SNMP Supported Protocols Detection	✗	

Hosts

Host	Services	OS
192.168.30.1	8	🖥️
192.168.20.7	2	🐧
192.168.20.37	0	🖥️
192.168.20.36	0	🖥️
192.168.20.34	0	🖥️
192.168.20.33	0	🖥️
192.168.20.32	2	🖥️

Vulnerabilities

14	26	58	25	44	0
CRITICAL	HIGH	MED	LOW	INFO	UNCLASSIFIED

Workspace's worth

👛 \$218,500.00 total

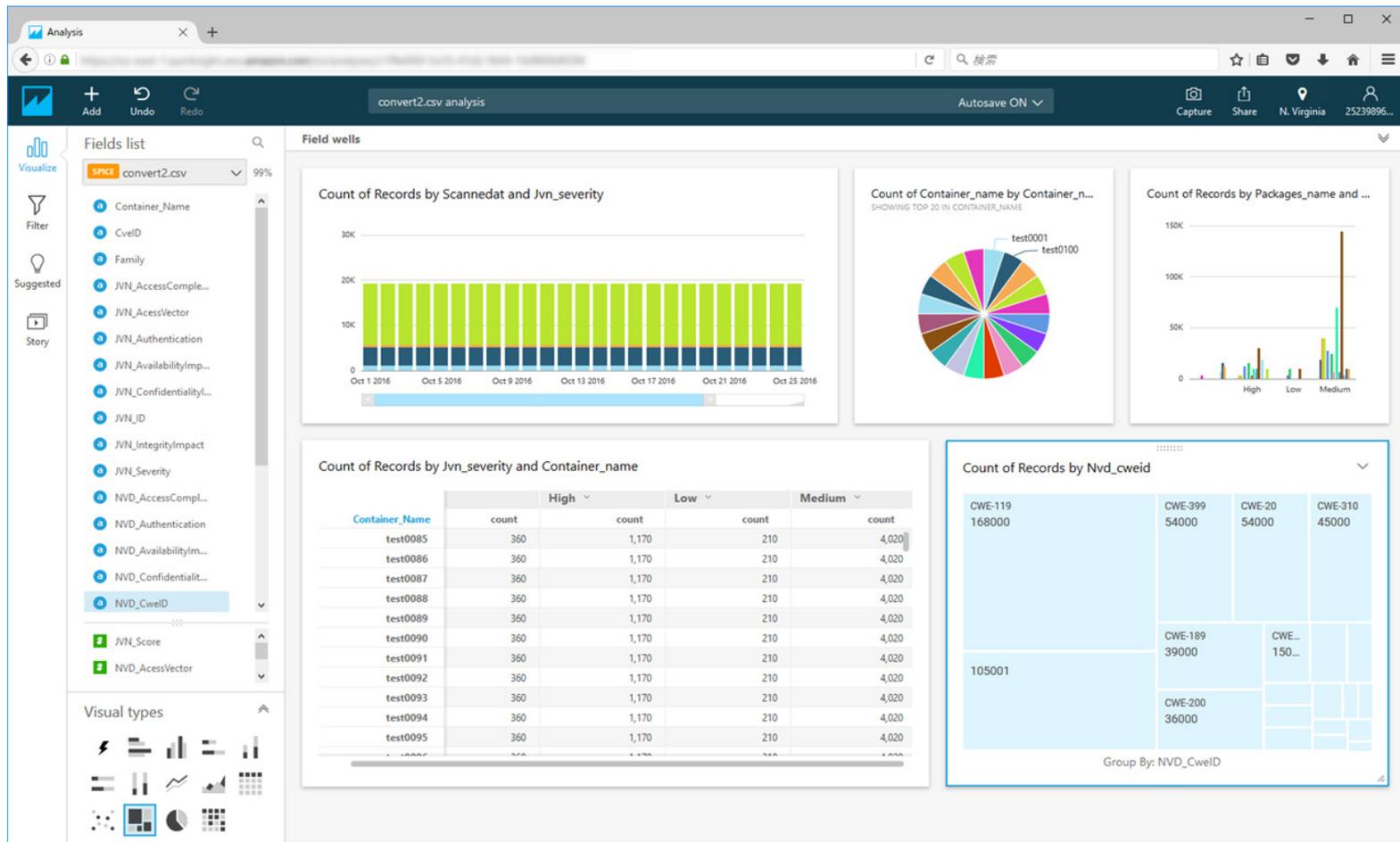
critical \$ 5000	high \$ 3000	med \$ 1000	low \$ 500	info \$ 0	unclassified \$ 0
------------------	--------------	-------------	------------	-----------	-------------------

Commands History

By	Command	Start Date	Duration
mica@rama	nmap 127.0.0.1	12/16/2015 at 8:11PM	0.17s
mica@rama	nmap 127.0.0.1	12/16/2015 at 8:06PM	0.14s
mica@rama	nmap -oX /home/mica/faraday/data/a2_Nmap_output-2.64496519857.xml 127.0.0.1	12/16/2015 at 8:05PM	0.13s
mica@rama	./plugin -f getAllIps.py	11/11/2015 at 5:27PM	0.12s

AWS Quicksight

- AWSのBIツールを使ってダッシュボードを作った例



Vuls TUI

- ターミナルUIがVuls本体に付属している

```
172-31-4-82 [ 1] CVE-2016-0494 | 10.0(High) | Unspecified vulnerability in the Java SE and Java SE Embedded components in
[ 2] CVE-2016-0483 | 10.0(High) | Unspecified vulnerability in the Java SE, Java SE Embedded, and JRockit comp
[ 3] CVE-2016-0799 | 10.0(High) | The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s a
[ 4] CVE-2016-0705 | 10.0(High) | Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_
[ 5] CVE-2016-0728 | 7.2 (High) | The join_session_keyring function in security/keys/process_keys.c in the Lin
[ 6] CVE-2016-1950 | 6.8 (Medium) | Heap-based buffer overflow in Mozilla Network Security Services (NSS) before
[ 7] CVE-2016-0778 | 6.5 (Medium) | The (1) roaming_read and (2) roaming_write functions in roaming_common.c in
[ 8] CVE-2016-0723 | 5.6 (Medium) | Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linu

CVE-2016-0705
=====
CVSS Score
-----
10.0 (High) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Summary
-----
Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1
.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or poss
ibly have unspecified other impact via a malformed DSA private key.
Package/CPE
-----
* openssl-1.0.1k-10.87.amzn1 -> openssl-1:1.0.1k-14.90.amzn1
Links
-----
* [NVD]( https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0705 )
* [MITRE]( https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0705 )
* [CveDetails]( http://www.cvedetails.com/cve/CVE-2016-0705 )
* [CVSSv2 Calculator]( https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2016-0705&vector=(AV:N/AC:L/Au:N/C:C/I
:C/A:C) )
* [RHEL-CVE]( https://access.redhat.com/security/cve/CVE-2016-0705 )
* [ALAS-2016-661]( https://alas.aws.amazon.com/ALAS-2016-661.html )
References
```

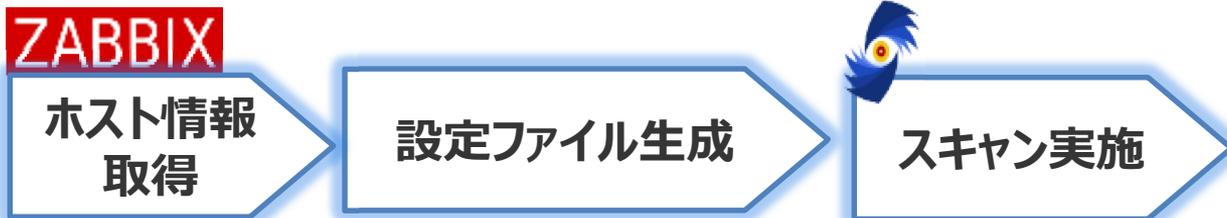
他ツールとの連携

Zabbixとの連携

Qiita:脆弱性スキャナVulsのスキャン結果をZabbixへ連携しアラート通知する



Qiita:Zabbixに登録されたホスト情報を脆弱性スキャナVulsへ自動連携する



他ツールとの連携

AWSとの連携

Qiita:脆弱性スキャナVulsでEC2をスキャンし脆弱性深刻度をタグ付け

Name	vuls	インスタンスタ...	アベイラビリティ...	インスタンスの...	ステータスチェッ...	アラームのステ...
amazon1	High	t2.nano	ap-northeast-1b	● running	✔ 2/2 のチェッ..	なし



JSONをS3に出力



Lambda実行
EC2にタグ付

EC2のVulsスキャンをほんの少し便利にするツール「ec2-vuls-config」

Ec2-vuls-configを実行

タグを指定してVuls設定ファイル生成



生成された設定ファイルを使ってスキャン

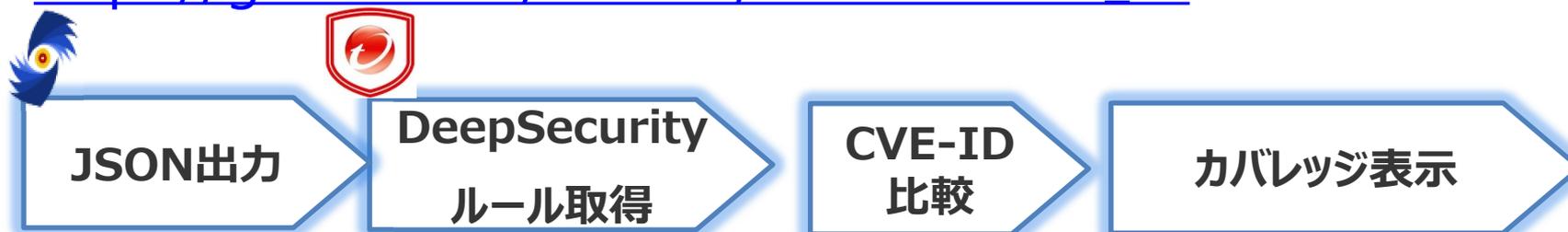
他ツールとの連携

Redmineと連携した脆弱性対策のワークフロー



Trend Micro Deep Security ルールのカバレッジ表示

https://github.com/kn0630/vulssimulator_ds



活発な開発

- 半年間で [182](#) 個の機能拡張、バグフィックス(2016/11/15)
 - ✓ FreeBSD Support by [justyntemme #90](#)
 - ✓ High Speed Scanning on CentOS by [ti-ga #138](#)
 - ✓ High speed data fetch from JVN by [kotakanbe #21](#)
 - ✓ High speed scanning on Ubuntu(20x Faster on Ubuntu, 4x Faster on Debian) by [kotakanbe #172](#)
 - ✓ Setup Vuls using DockerHub by [matsuno #223](#)
 - ✓ Add support for reading CVE data from MySQL. by [oswell #225](#)
 - ✓ Integrate OWASP Dependency Check [#232](#)
 - ✓ ...

Vuls vs OpenVAS vs AWS Inspector

[Qiita: Vuls・OpenVAS・Amazon Inspectorを徹底比較](#)

今後の課題

スキャンの検知精度の向上

- 現状Ubuntu/Debian/CentOSはチェンジログを解析
チェンジログの記述次第で検知漏れの可能性があるため、
バージョン比較での検知ロジックを併用し精度を向上させる

大規模環境対応

- 数千台、数万台規模を想定したチューニング

他の脆弱性スキャナとの連携

- 設定、状態までを考慮した賢いスキャン
- サーバ設定Audit系
- WordPressプラグイン用脆弱性スキャナなど

Vulsの参考情報

- GitHub VulsのREADMEが充実
 - ✓ [日本語のREADME](#)
- [Qiita: 脆弱性スキャナVuls 関連リンク集](#)
- Vuls祭り #1 2016/9/26 開催 100名ほど参加
 - ✓ [Slides@connpass](#)
- [Qiita: Vuls Advent Calendar 2016](#)
- Join Slack Team 参加者263名（日本語チャンネルは138名）
 - ✓ <http://bit.ly/2ft8H5c>

サーバのソフトウェアアップデートは必要です

- IPS/IDS, Antivirusでは防げない脆弱性が存在します
- ツールを使ってシステムに潜在する脆弱性を見える化しましょう

Vulsは継続的な脆弱性対策を可能にします

- 新規に脆弱性やアップデートが公開されたタイミングで、脆弱性の詳細情報と該当するサーバをVulsが教えてくれます

OSSなので明日から**無料**で使えます！

有償サポートやカスタマイズはご相談ください

- フューチャーアーキテクト株式会社 担当：神戸（かんべ）まで
- [mailto: gr-tig-ta-security@future.co.jp](mailto:gr-tig-ta-security@future.co.jp)