

Vuls & VulsRepo: A Highly Flexible Vulnerability Scanner and Visualizer

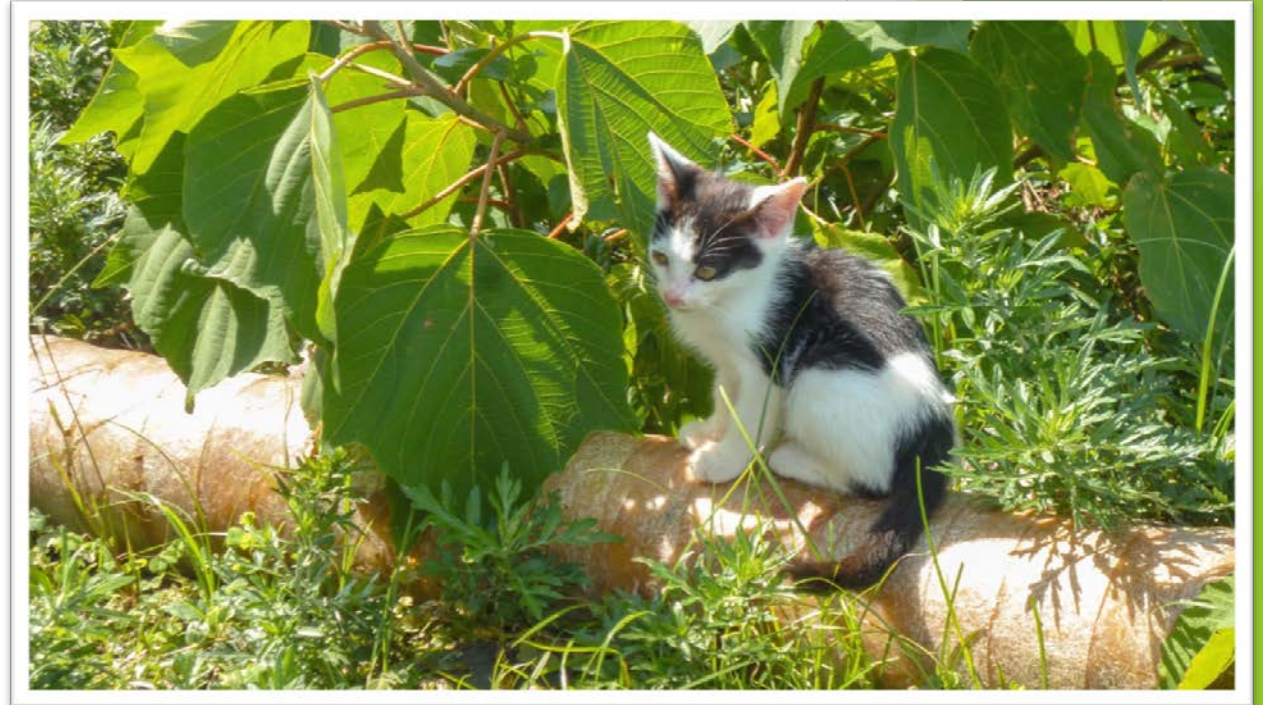
Yasunari Momoi momo@ijj.ad.jp

Internet Initiative Japan Inc.

Apricot 2018

Agenda

- ▶ What is Vuls?
- ▶ How it works
- ▶ Visualization with VulsRepo
- ▶ Reporting in local language
- ▶ (near) future work



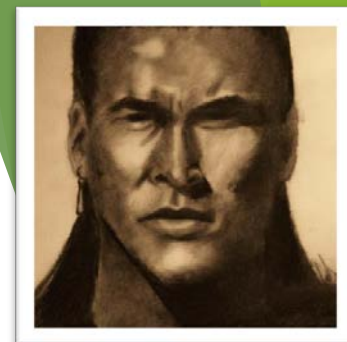
About me

- ▶ momo: Yasunari Momoi
 - ▶ Internet Initiative Japan Inc., IIJ-SECT member
 - ▶ Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division
 - ▶ Facebook ymomoi Twitter @sbg
- ▶ Software Developer, Network Engineer, Server Engineer, Security, SOC/CSIRT
 - ▶ Supporting some Open Source Software and User Community
- ▶ Special Interest
 - ▶ various kind of foods, local foods
 - ▶ Heavy Metal / Hard Rock Music
 - ▶ Cats!



Vuls: VULnerability Scanner

- ▶ Vuls is the VULnerability Scanner written in go language.
 - ▶ Develop by community: Vuls dev team
 - ▶ Main developer: Kota Kanbe @kotakanbe
 - ▶ Also supported by Future Architect, Inc.
- ▶ Open Source Software
 - ▶ GPL v3.0
- ▶ Distribute with Docker image
- ▶ <https://vuls.io/>



Agentless Vulnerability Scanner for Linux/FreeBSD

TUTORIAL

SUPPORTED OS

GITHUB

Vuls is open-source, agent-less vulnerability scanner based on information from NVD, OVAL, etc.

Vuls: main feature (1)

- ▶ Vuls supports many kinds of Linux/FreeBSD systems
 - ▶ Alpine Linux, Ubuntu, Debian, CentOS
 - ▶ Amazon Linux, RedHat Enterprise Linux, Oracle Linux, SUSE Enterprise Linux
 - ▶ Raspbian
 - ▶ FreeBSD
- ▶ High flexibility
 - ▶ scans local/remote machine
 - ▶ scans system inside Docker container
 - ▶ works in an isolated network (without the Internet connectivity)



Vuls: main feature (2)

- ▶ To improve accuracy, Vuls uses various public information sources
 - ▶ NVD/CVE
 - ▶ Vendor information
 - ▶ OVAL (RedHat, Debian, Ubuntu, SUSE, Oracle Linux)
 - ▶ Alpine secdb
 - ▶ RHSA/ALAS/ELSA/FreeBSD-SA
 - ▶ ChangeLog
 - ▶ JVN (Japan Vulnerability Notes in Japanese language)



Vuls: main feature (3)

- ▶ Optionally, scanning non-OS packages
 - ▶ using configuration file and CPE information
 - ▶ using output from OWASP Dependency Check
- ▶ Scanning results to Email/Slack
- ▶ Reports in local language
 - ▶ Japanese users can refer JVN database :D



Vuls: scanning and reporting example

```
3. vuls@vuls-sv-centos7:~ (ssh)
X sanctuary2 (zsh) %1 X sanctuary2 (zsh) %2 X vuls@vuls-sv-ce... %3

[vuls@vuls-sv-centos7 ~]$ vuls scan -config config.toml -results-dir /opt/vuls/
results -log-dir /opt/vuls/log -http-proxy http://proxy.
[Feb 21 12:47:29] INFO [localhost] Start scanning
[Feb 21 12:47:29] INFO [localhost] config: config.toml
[Feb 21 12:47:29] INFO [localhost] Validating config...
[Feb 21 12:47:29] INFO [localhost] Detecting Server/Container OS...
[Feb 21 12:47:29] INFO [localhost] Detecting OS of servers...
[Feb 21 12:47:29] INFO [localhost] (1/3) Detected: vuls-debian8: debian 8.6
[Feb 21 12:47:29] INFO [localhost] (2/3) Detected: vuls-ubuntu16: ubuntu 16.04
[Feb 21 12:47:35] INFO [localhost] (3/3) Detected: vuls-centos7: centos 7.2.15
1
[Feb 21 12:47:35] INFO [localhost] Detecting OS of containers...
[Feb 21 12:47:35] INFO [localhost] Detecting Platforms...
[Feb 21 12:47:51] INFO [localhost] (1/3) vuls-debian8 is running on other
[Feb 21 12:47:51] INFO [localhost] (2/3) vuls-centos7 is running on other
[Feb 21 12:47:51] INFO [localhost] (3/3) vuls-ubuntu16 is running on other
[Feb 21 12:47:51] INFO [localhost] Scanning vulnerabilities...
[Feb 21 12:47:51] INFO [localhost] Scanning vulnerable OS packages...

One Line Summary
=====
vuls-ubuntu16  ubuntu16.04      226 updatable packages
vuls-debian8   debian8.6          102 updatable packages
vuls-centos7   centos7.2.1511    244 updatable packages

To view the detail, vuls tui is useful.
To send a report, run vuls report -h.
[vuls@vuls-sv-centos7 ~]$
```

```
3. vuls@vuls-sv-centos7:~ (ssh)
X sanctuary2 (zsh) %1 X sanctuary2 (zsh) %2 X vuls@vuls-sv-centos... %3

vuls-centos7 (centos7.2.1511)
vuls-debian8 (debian8.6)
vuls-ubuntu16 (ubuntu16.04)

[ 1] CVE-2015-2806 | 10.0 | 100 | Stack-based buffer overflow in asn1_der_decoding in
[ 2] CVE-2015-8812 | 10.0 | 100 | drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux
[ 3] CVE-2016-5636 | 10.0 | 100 | Integer overflow in the get_data function in zipimp
[ 4] CVE-2016-6662 | 10.0 | 100 | Oracle MySQL through 5.5.52, 5.6.x through 5.6.33,
[ 5] CVE-2016-7117 | 10.0 | 100 | Use-after-free vulnerability in the __sys_recvmmsg
[ 6] CVE-2016-9555 | 10.0 | 100 | The sctp_sf_ootb function in net/sctp/sm_statefuns.
[ 7] CVE-2017-7895 | 10.0 | 100 | The NFSv2 and NFSv3 server implementations in the L
[ 8] CVE-2017-8890 | 10.0 | 100 | The inet_csk_clone_lock function in net/ipv4/inet_c

CVE-2016-6662
=====

CVSS Scores
-----
IMPORTANT 8.0/CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H redhat
HIGH      10.0/AV:N/AC:L/Au:N/C:C/I:C/A:C nvd
IMPORTANT 7.1/AV:N/AC:H/Au:S/C:C/I:C/A:C redhat
HIGH      10.0/AV:N/AC:L/Au:N/C:C/I:C/A:C jvn

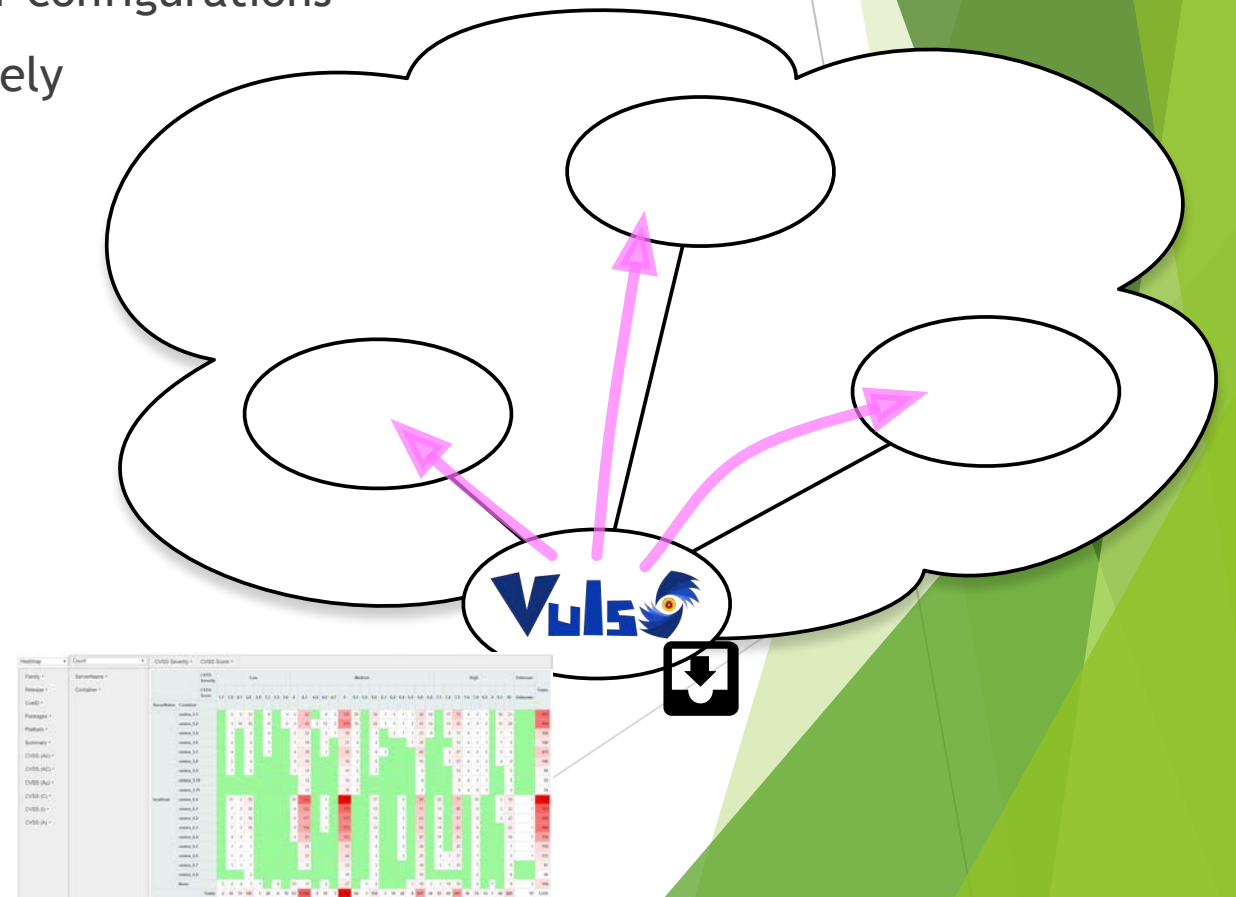
Summary
-----
Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x thr
ough 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10
.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x
before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users
to create arbitrary configurations and bypass certain protection
mechanisms by setting general_log_file to a my.cnf configuration.
NOTE: this can be leveraged to execute arbitrary code with root
privileges by setting malloc_lib. NOTE: the affected MySQL versio
n information is from Oracle's October 2016 CPU. Oracle has not c
ommented on third-party claims that the issue was silently patche
d in MySQL 5.5.52, 5.6.33, and 5.7.15. (nvd)

Links
-----
* https://nvd.nist.gov/vuln/detail/CVE-2016-6662
* https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2
016-6662

mariadb-libs-1:5.5.44-2.el7.centos -> 1:5.5.56-2.el7
-----
```

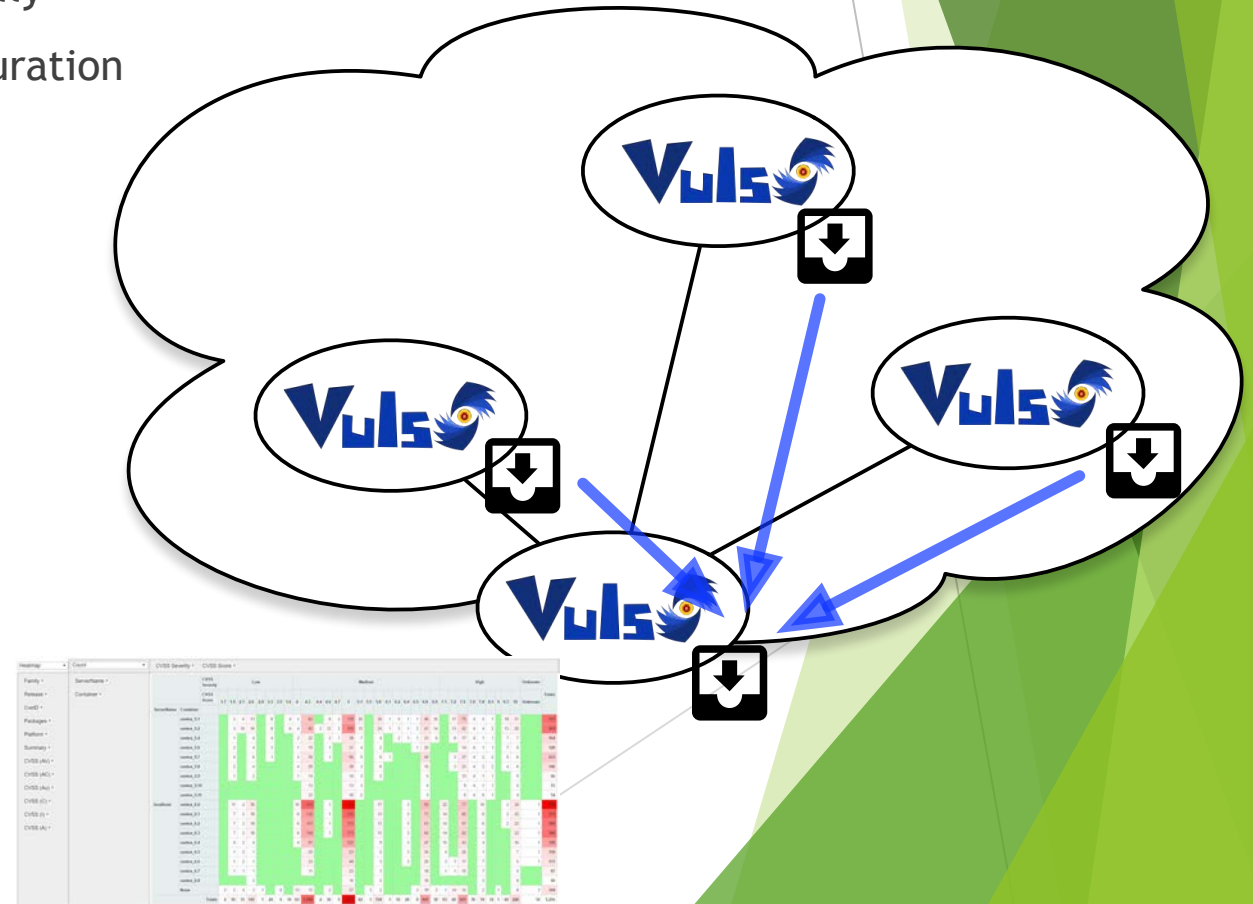

Vuls: flexibility (1)

- ▶ Vuls can be worked on various network / server configurations
- ▶ Case 1: Install Vuls on one host and scan remotely



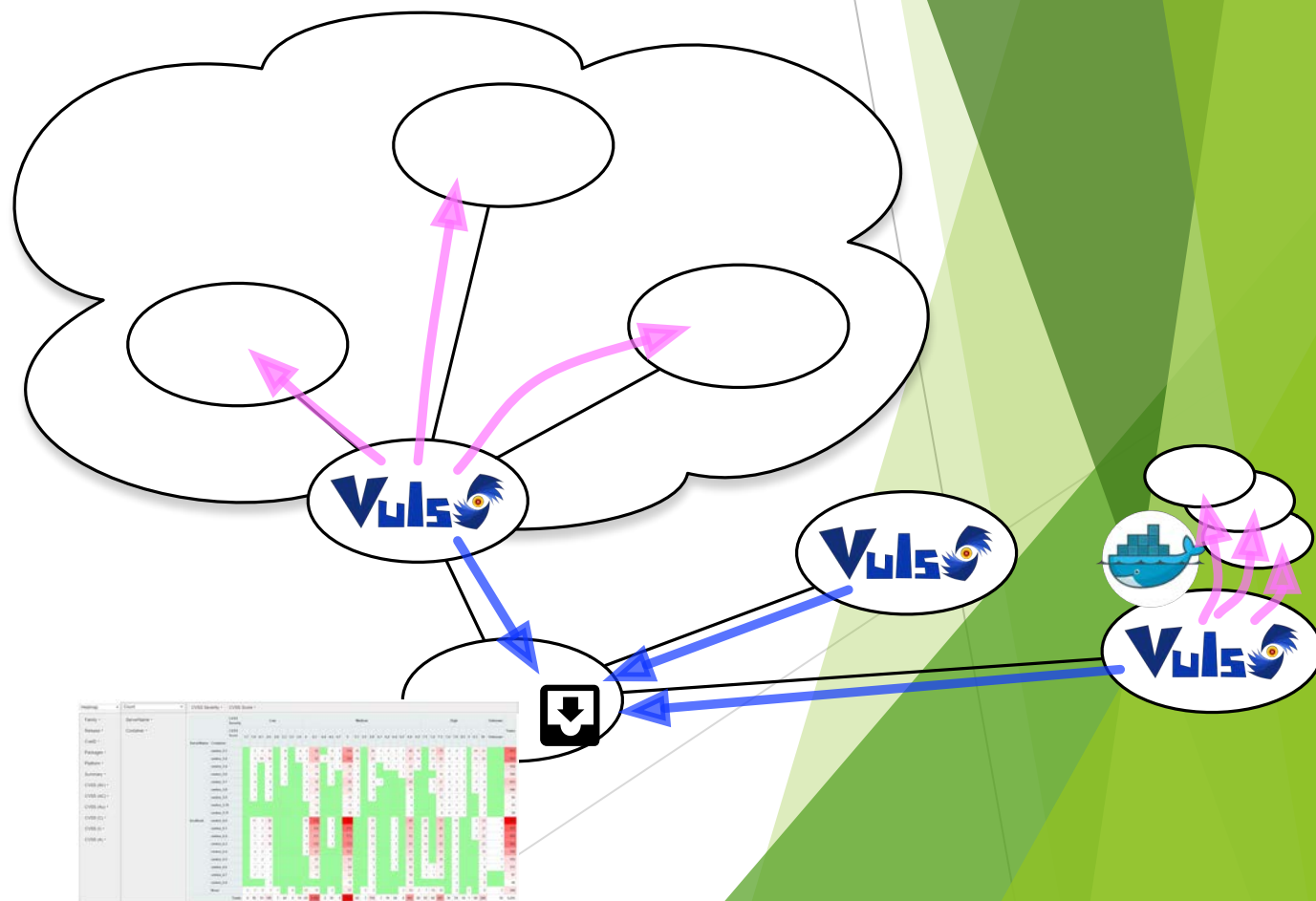
Vuls: flexibility (2)

- ▶ Case 2: Install Vuls on all hosts and scan locally
 - ▶ Just copying single executable file and configuration
 - ▶ Vuls outputs result in single JSON file



Vuls: flexibility (3)

- ▶ Case 3: Hybrid remote and local scan
 - ▶ Vuls can scan inside Docker container
 - ▶ You can collect result file using any method



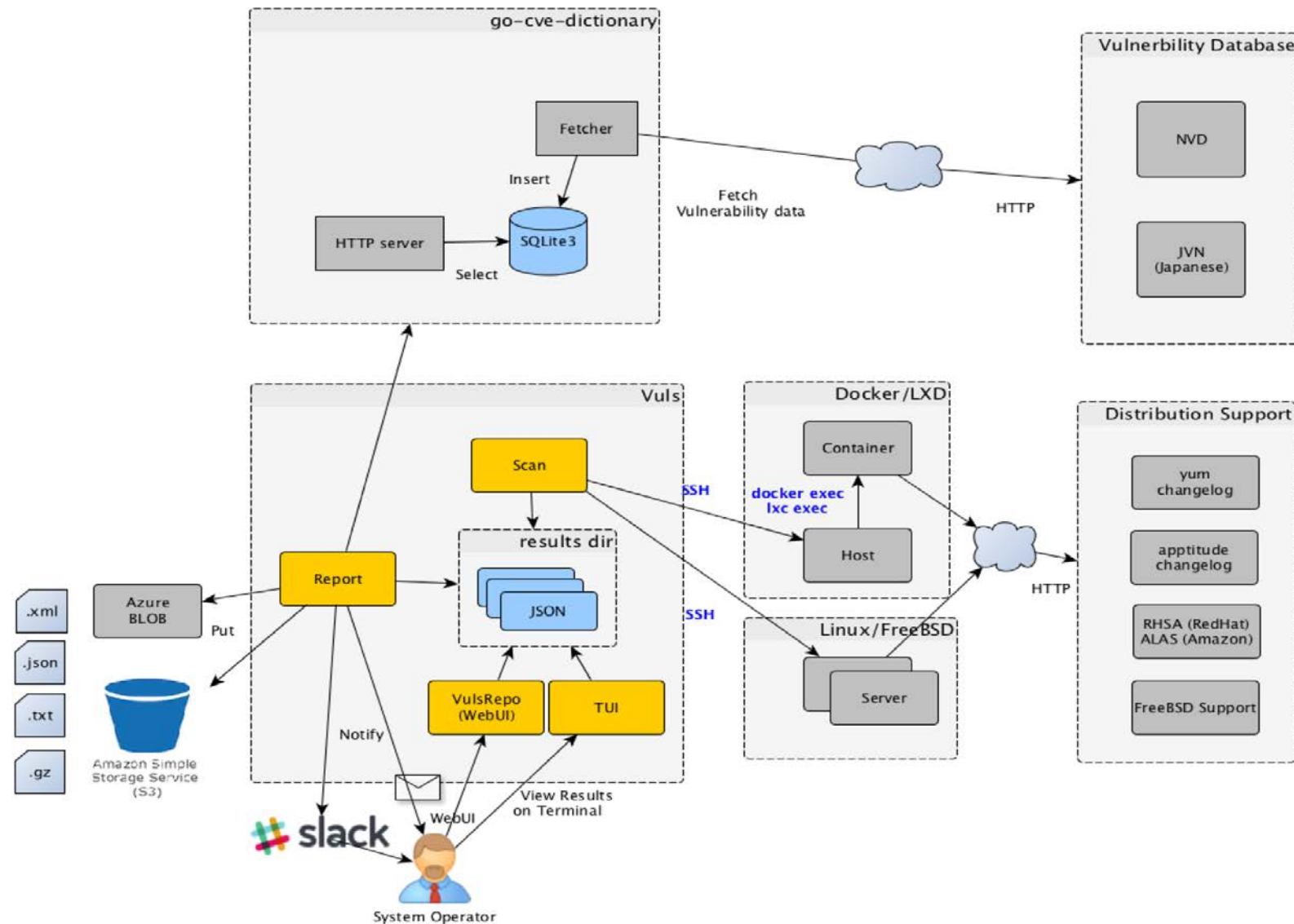
Vuls: flexibility (4)

- ▶ Just single executable file
 - ▶ because written in go language
 - ▶ easy to use on any host (just copying!)
- ▶ Output is simple JSON file
 - ▶ no server, no database host required
 - ▶ you can view scanning results at any host (just copying!)
 - ▶ you can copy/merge results



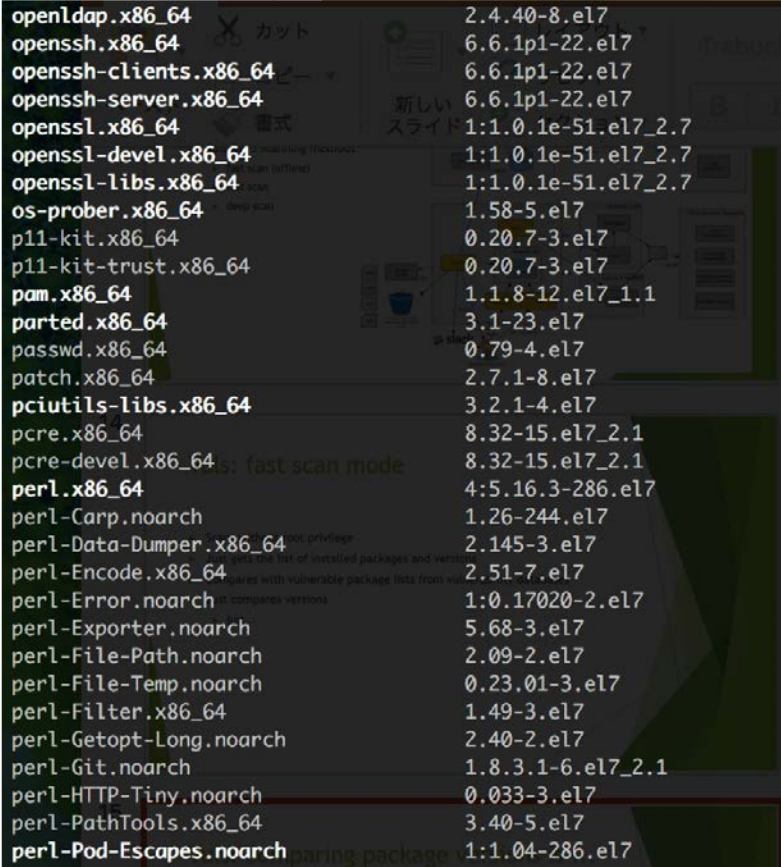
Vuls: scanning methods

- ▶ Vuls has 3 scanning methods
 - ▶ fast scan (offline)
 - ▶ fast scan
 - ▶ deep scan



Vuls: fast scan mode

- ▶ Scans without root privilege (except Raspbian)
- ▶ Just gets the list of installed packages and versions
- ▶ Compares with vulnerable package lists from vulnerability databases
- ▶ Just compares versions
 - ▶ just...



```
openldap.x86_64 2.4.40-8.el7
openssh.x86_64 6.6.1p1-22.el7
openssh-clients.x86_64 6.6.1p1-22.el7
openssh-server.x86_64 6.6.1p1-22.el7
openssl.x86_64 1:1.0.1e-51.el7_2.7
openssl-devel.x86_64 1:1.0.1e-51.el7_2.7
openssl-libs.x86_64 1:1.0.1e-51.el7_2.7
os-prober.x86_64 1.58-5.el7
p11-kit.x86_64 0.20.7-3.el7
p11-kit-trust.x86_64 0.20.7-3.el7
pam.x86_64 1.1.8-12.el7_1.1
parted.x86_64 3.1-23.el7
passwd.x86_64 0.79-4.el7
patch.x86_64 2.7.1-8.el7
pciutils-libs.x86_64 3.2.1-4.el7
pcre.x86_64 8.32-15.el7_2.1
pcre-devel.x86_64 8.32-15.el7_2.1
perl.x86_64 4:5.16.3-286.el7
perl-Carp.noarch 1.26-244.el7
perl-Data-Dumper.x86_64 2.145-3.el7
perl-Encode.x86_64 2.51-7.el7
perl-Error.noarch 1:0.17020-2.el7
perl-Exporter.noarch 5.68-3.el7
perl-File-Path.noarch 2.09-2.el7
perl-File-Temp.noarch 0.23.01-3.el7
perl-Filter.x86_64 1.49-3.el7
perl-Getopt-Long.noarch 2.40-2.el7
perl-Git.noarch 1.8.3.1-6.el7_2.1
perl-HTTP-Tiny.noarch 0.033-3.el7
perl-PathTools.x86_64 3.40-5.el7
perl-Pod-Escapes.noarch 1:1.04-286.el7
```

Vuls: comparing package versions is ...

- ▶ It is “a little bit” tough
- ▶ We understand managing package and versioning is a tough task
- ▶ Version numbering is in chaos
 - ▶ Implements all cases
 - ▶ He did!

```
libgssapi3-heimdal/xenial,now 1.7~git20150920+dfsg-4ubuntu1.16.04.1 [installed,upgradable to: 1.7~git20150920+dfsg-4ubuntu1.16.04.1]
libhcrypto4-heimdal/xenial,now 1.7~git20150920+dfsg-4ubuntu1.16.04.1 [installed,upgradable to: 1.7~git20150920+dfsg-4ubuntu1.16.04.1]
libheimbase1-heimdal/xenial,now 1.7~git20150920+dfsg-4ubuntu1.16.04.1 [installed,upgradable to: 1.7~git20150920+dfsg-4ubuntu1.16.04.1]
libheimntlm0-heimdal/xenial,now 1.7~git20150920+dfsg-4ubuntu1.16.04.1 [installed,upgradable to: 1.7~git20150920+dfsg-4ubuntu1.16.04.1]
libhogweed4/xenial,now 3.2-1 amd64 [installed,upgradable to: 3.2-1]
libhx509-5-heimdal/xenial,now 1.7~git20150920+dfsg-4ubuntu1.16.04.1 [installed,upgradable to: 1.7~git20150920+dfsg-4ubuntu1.16.04.1]
libicu55/xenial,now 55.1-7 amd64 [installed,upgradable to: 55.1-7]
libidn11/norow 1.32-3ubuntu1.1 amd64 [installed,upgradable to: 1.32-3ubuntu1.1]
libisc-export160/norow 1:9.10.3.dfsg.P4-8ubuntu1.2 amd64 [installed,upgradable to: 1:9.10.3.dfsg.P4-8ubuntu1.2]
libisc160/norow 1:9.10.3.dfsg.P4-8ubuntu1.2 amd64 [installed,upgradable to: 1:9.10.3.dfsg.P4-8ubuntu1.2]
libisccc140/norow 1:9.10.3.dfsg.P4-8ubuntu1.2 amd64 [installed,upgradable to: 1:9.10.3.dfsg.P4-8ubuntu1.2]
libiscfg140/norow 1:9.10.3.dfsg.P4-8ubuntu1.2 amd64 [installed,upgradable to: 1:9.10.3.dfsg.P4-8ubuntu1.2]
libisl15/xenial,now 0.16.1-1 amd64 [installed,automatic]
libitm1/xenial-security,now 5.4.0-6ubuntu1~16.04.4 amd64 [installed,upgradable to: 5.4.0-6ubuntu1~16.04.4]
libjson-c2/xenial,now 0.11-4ubuntu2 amd64 [installed]
libk5crypto3/xenial,now 1.13.2+dfsg-5 amd64 [installed,upgradable to: 1.13.2+dfsg-5]
libkeyutils1/xenial,now 1.5.9-8ubuntu1 amd64 [installed]
```

```
openldap.x86_64 2.4.40-8.el7
openssh.x86_64 6.6.1p1-22.el7
openssh-clients.x86_64 6.6.1p1-22.el7
openssh-server.x86_64 6.6.1p1-22.el7
openssl.x86_64 1:1.0.1e-51.el7_2.7
openssl-devel.x86_64 1:1.0.1e-51.el7_2.7
openssl-libs.x86_64 1:1.0.1e-51.el7_2.7
os-prober.x86_64 1.58-5.el7
p11-kit.x86_64 0.20.7-3.el7
p11-kit-trust.x86_64 0.20.7-3.el7
pam.x86_64 1.1.8-12.el7_1.1
parted.x86_64 3.1-23.el7
passwd.x86_64 0.79-4.el7
patch.x86_64 2.7.1-8.el7
pciutils-libs.x86_64 3.2.1-4.el7
pcpre.x86_64 8.32-15.el7_2.1
pcpre-devel.x86_64 8.32-15.el7_2.1
perl.x86_64 4:5.16.3-286.el7
perl-Carp.noarch 1.26-244.el7
perl-Data-Dumper.x86_64 2.145-3.el7
perl-Encode.x86_64 2.51-7.el7
perl-Error.noarch 1:0.17020-2.el7
perl-Exporter.noarch 5.68-3.el7
perl-File-Path.noarch 2.09-2.el7
perl-File-Temp.noarch 0.23.01-3.el7
perl-Filter.x86_64 1.49-3.el7
perl-Getopt-Long.noarch 2.40-2.el7
perl-Git.noarch 1.8.3.1-6.el7_2.1
perl-HTTP-Tiny.noarch 0.033-3.el7
perl-PathTools.x86_64 3.40-5.el7
perl-Pod-Escapes.noarch 1:1.04-286.el7
```

3.6.20-1.ab1 [?] \leq 3.6.20-1.2



3.6.20-1.ab1 $>$ 3.6.20-1.2

3.6.20-1.ab1 $<$ 3.6.20-1.2

Debian

Red Hat

Vuls: deep scan mode

- ▶ Needs root privileges (on some OSes)
- ▶ Slow
- ▶ Crawls additional data from installed packages if available
 - ▶ ChangeLog
- ▶ Why process ChangeLog?
 - ▶ ChangeLog is written directly by the developer
 - ▶ It seems to be relatively credible?
 - ▶ Security fix logline has relevant CVE ID



Vuls: improving detecting accuracy

- ▶ Vulnerability databases sometimes...
 - ▶ miss related CVE ID
 - ▶ take time to update their contents
 - ▶ lack of affected systems
- ▶ Vuls uses as much information about patches/versions
 - ▶ In these case, Vuls can find vulnerable module from other data sources
- ▶ I think this is a cool idea! :D

One Line Summary

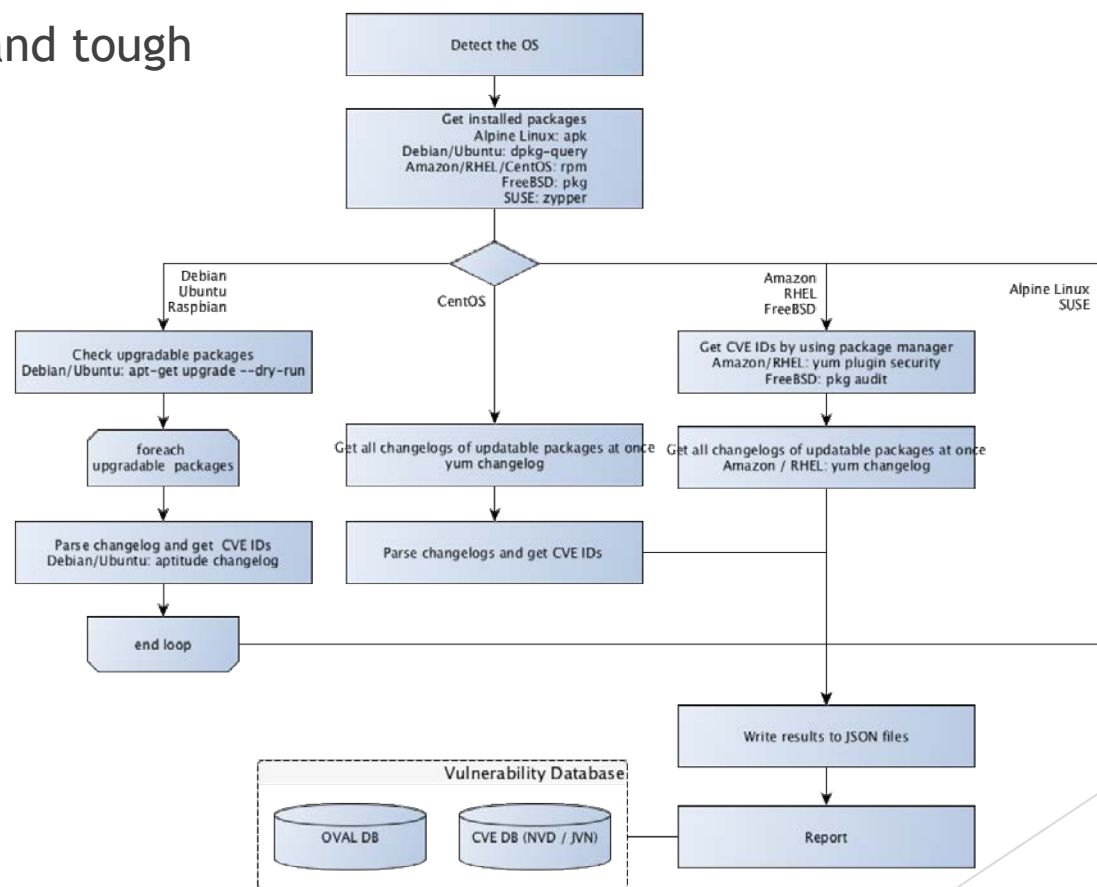
vuls-centos7	Total: 274 (High:80 Medium:165 Low:29 ?:0)	209 updatable packages
vuls-debian8	Total: 57 (High:6 Medium:44 Low:2 ?:5)	102 updatable packages
vuls-ubuntu16	Total: 83 (High:52 Medium:26 Low:5 ?:0)	177 updatable packages

One Line Summary (deep scan)

vuls-centos7	Total: 305 (High:89 Medium:184 Low:32 ?:0)	209 updatable packages
vuls-debian8	Total: 298 (High:70 Medium:183 Low:16 ?:29)	102 updatable packages
vuls-ubuntu16	Total: 165 (High:88 Medium:61 Low:8 ?:8)	177 updatable packages

Vuls: supports many distributions

- ▶ System commands around packaging are different between distributions
- ▶ It is troublesome and tough
 - ▶ But we did!



Supported OS

DISTRIBUTION	RELEASE
Alpine	3.2 and later
Ubuntu	14, 16
Debian	7, 8, 9
RHEL	5, 6, 7
Oracle Linux	5, 6, 7
CentOS	6, 7
Amazon Linux	All
FreeBSD	10, 11
SUSE Enterprise	11, 12
Raspbian	Jessie, Stretch

Vuls: reporting

- ▶ Vuls output results to simple JSON format file
 - ▶ easy to feed into other systems (DB, ticketing, etc.)
- ▶ Notify by Email and/or Slack when scanning is completed
 - ▶ reporting summary
- ▶ Result can be read by TUI
 - ▶ I recommend using VulsRepo

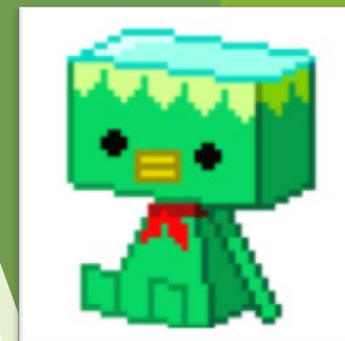
```
3. vuls@vuls-sv-centos7:~ (ssh)
X sanctuary2 (zsh)  %1 X sanctuary2 (zsh)  %2 X vuls@vuls-sv-centos... %3
vuls-centos7 (centos7.2.1511) [ 1] CVE-2015-2806 | 10.0 | 100 | Stack-based buffer overflow in asn1_der_decoding in
vuls-debian8 (debian8.6) [ 2] CVE-2015-8812 | 10.0 | 100 | drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux
vuls-ubuntu16 (ubuntu16.04) [ 3] CVE-2016-5636 | 10.0 | 100 | Integer overflow in the get_data function in zipimp
[ 4] CVE-2016-6662 | 10.0 | 100 | Oracle MySQL through 5.5.52, 5.6.x through 5.6.33,
[ 5] CVE-2016-7117 | 10.0 | 100 | Use-after-free vulnerability in the __sys_recvmmsg
[ 6] CVE-2016-9555 | 10.0 | 100 | The sctp_sf_ootb function in net/sctp/sm_statefuns.
[ 7] CVE-2017-7895 | 10.0 | 100 | The NFSv2 and NFSv3 server implementations in the L
[ 8] CVE-2017-8890 | 10.0 | 100 | The inet_csk_clone_lock function in net/ipv4/inet_c

CVE-2016-6662
=====
CVSS Scores
-----
IMPORTANT 8.0/CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H redhat
HIGH 10.0/AV:N/AC:L/Au:N/C:C/I:C/A:C nvd
IMPORTANT 7.1/AV:N/AC:H/Au:S/C:C/I:C/A:C redhat
HIGH 10.0/AV:N/AC:L/Au:N/C:C/I:C/A:C jvn

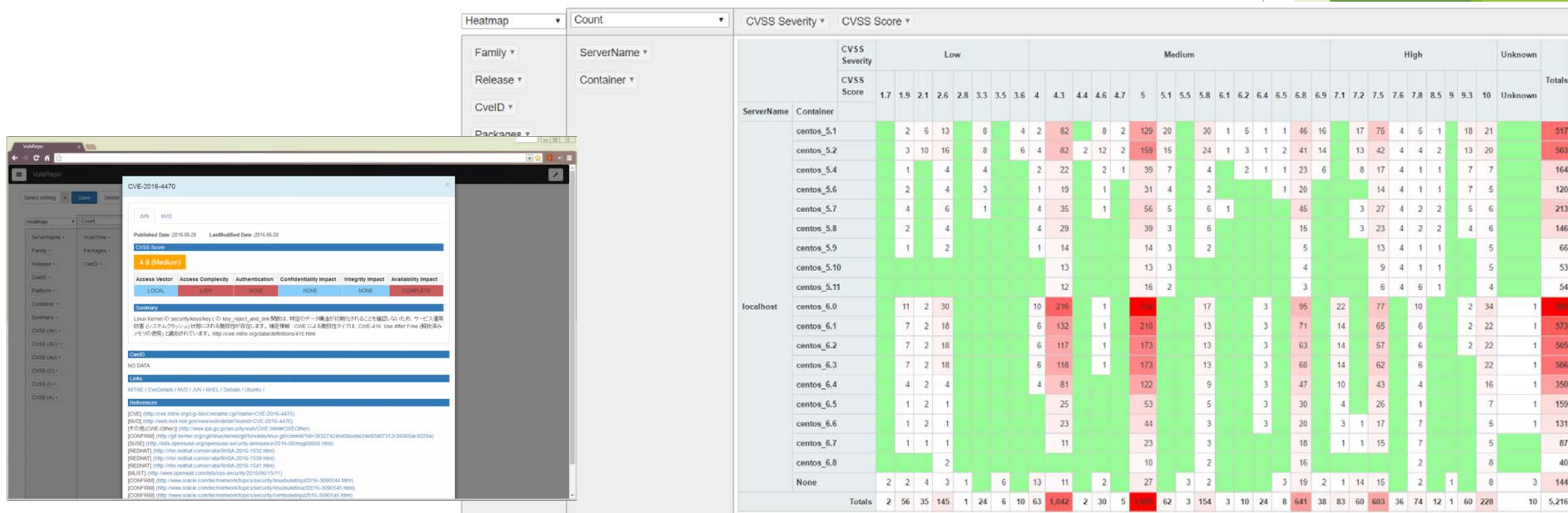
Summary
-----
Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x thr
ough 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10
.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x
before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users
to create arbitrary configurations and bypass certain protection
mechanisms by setting general_log_file to a my.cnf configuration.
NOTE: this can be leveraged to execute arbitrary code with root
privileges by setting malloc_lib. NOTE: the affected MySQL versio
n information is from Oracle's October 2016 CPU. Oracle has not c
ommented on third-party claims that the issue was silently patche
d in MySQL 5.5.52, 5.6.33, and 5.7.15. (nvd)

Links
-----
* https://nvd.nist.gov/vuln/detail/CVE-2016-6662
* https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2
016-6662
mariadb-libs-1:5.5.44-2.el7.centos -> 1:5.5.56-2.el7
```

VulsRepo: Visualizer of Vuls

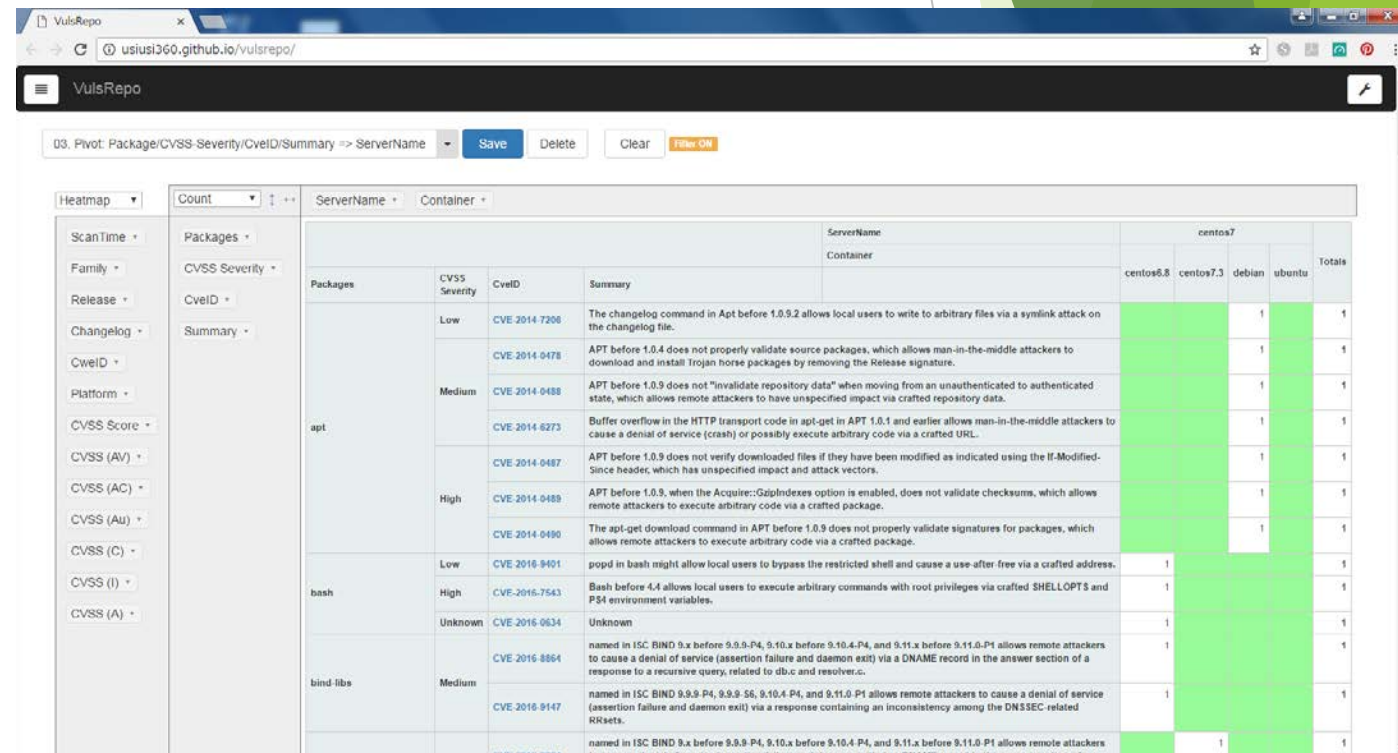


- ▶ Visualizer based on the Web
 - ▶ Main developer: Takayuki Ushida @usiusi360



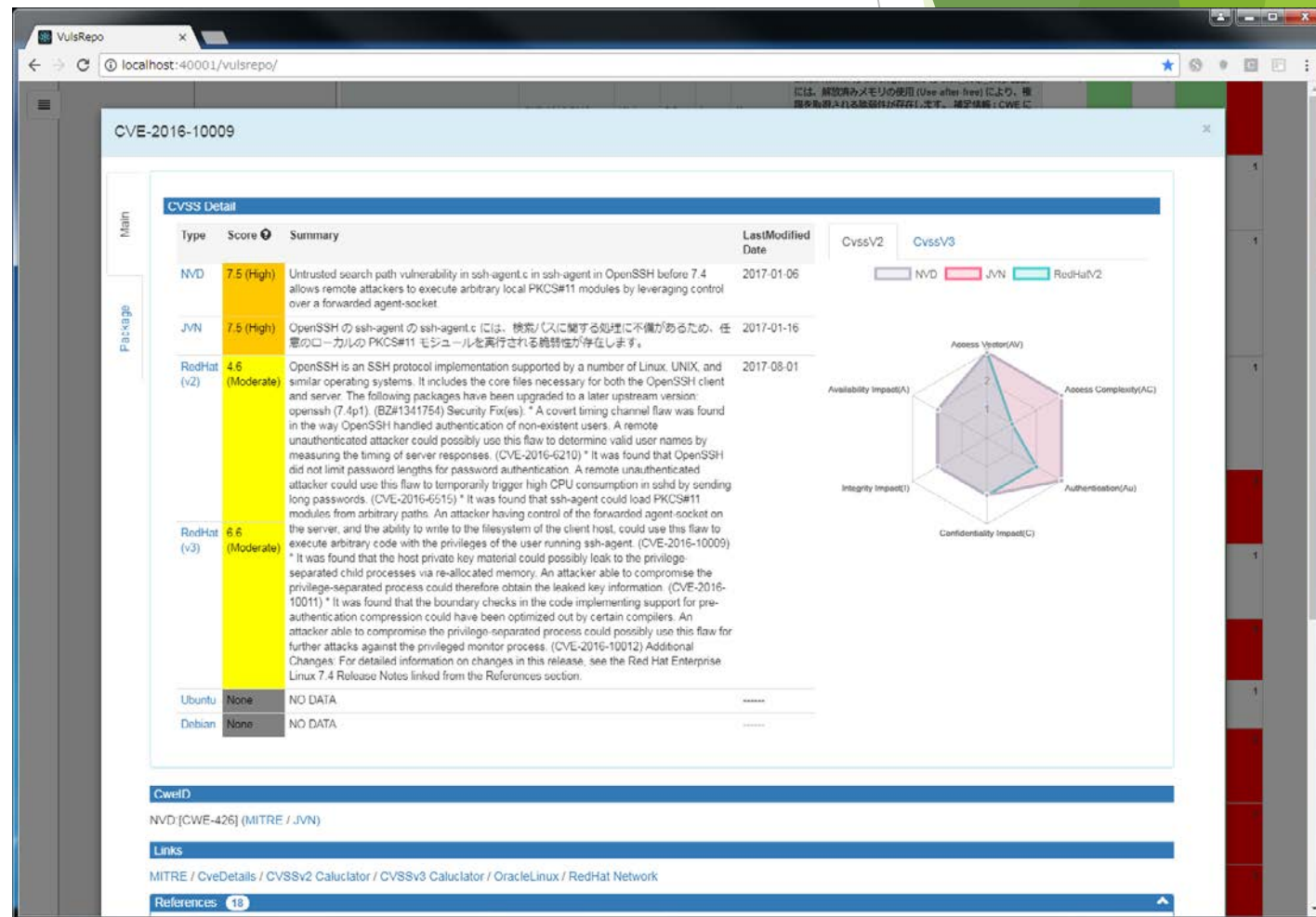
VulsRepo: Viewing scanning results

- ▶ Viewing charts with dynamic pivot table
 - ▶ coloring, filtering, etc.



VulsRepo: CVSS score viewer with chart

- ▶ You can read vulnerability description
 - ▶ Description summary
 - ▶ CVSS score
 - ▶ CVSSv2, CVSSv3 radar chart
 - ▶ related resource links



VulsRepo: viewing CVE and scan details

► CVE information and ChangeLog

The screenshot displays the VulsRepo web interface. A modal window for CVE-2016-7543 is open, showing the following details:

CveID	Confidence-DetectionMethod	Confidence-Score
CVE-2016-7543	ChangelogExactMatch	95

ServerName	ContainerName	PackageName
centos7	centos6.8	bash-4.1.2.40.el6 => 4.1.2.48.el6

Changelog

- *Wed Feb 15 12:00:00 2017 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-48
 - Fix signal handling in read builtinResolves: #1421926
- *Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-47
 - CVE-2016-9401 - Fix crash when '-' is passed as second sign to popdResolves: #1396383
- *Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-46
 - CVE-2016-7543 - Fix for arbitrary code execution via SHELLOPTS+PS4 variablesResolves: #1379630
- *Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-45
 - CVE-2016-0634 - Fix for arbitrary code execution via malicious hostnameResolves: #1377613
- *Fri Dec 9 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-44
 - Avoid crash in parameter expansion while expanding long stringsResolves: #1359142
- *Fri Dec 2 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-43
 - Stop reading input when SIGHUP is receivedResolves: #1325753

Reports in a local language

- ▶ Vuls and VulsRepo can show report in a local language
 - ▶ JVN (Japan Vulnerability Notes) DB has many records in Japanese
- ▶ Operators can read vulnerability reports in Japanese language!
 - ▶ It is very important for Japanese people ;)
- ▶ We can support any other local languages
 - ▶ but we don't know documentations in other languages
 - ▶ because we can't read them
- ▶ Please let me know information sources in your language
 - ▶ we will make it readable with Vuls and VulsRepo



(near) Future work

- ▶ More improvement in detection accuracy
 - ▶ Please let me know vulnerability information databases that we miss
- ▶ Scanning Cisco products with OVAL
 - ▶ Router, Switch, ...
 - ▶ PoC is working (written in Perl)
 - ▶ Accessing policy of network infrastructure is different from servers
 - ▶ I am thinking with implementation policy
- ▶ Report in your language
 - ▶ Please send request with the local resource information



Thanks!

- ▶ Vuls: <https://vuls.io/>
 - ▶ Join Slack: <http://goo.gl/forms/xm5KFo35tu>
- ▶ VulsRepo: <https://github.com/usiusi360/vulsrepo>

