

The Wayback Machine - <https://web.archive.org/web/20180901153521/https://vuls.io/> Search

Vuls

Docs

Community

Blog

Að English

GitHub

vulsdoc



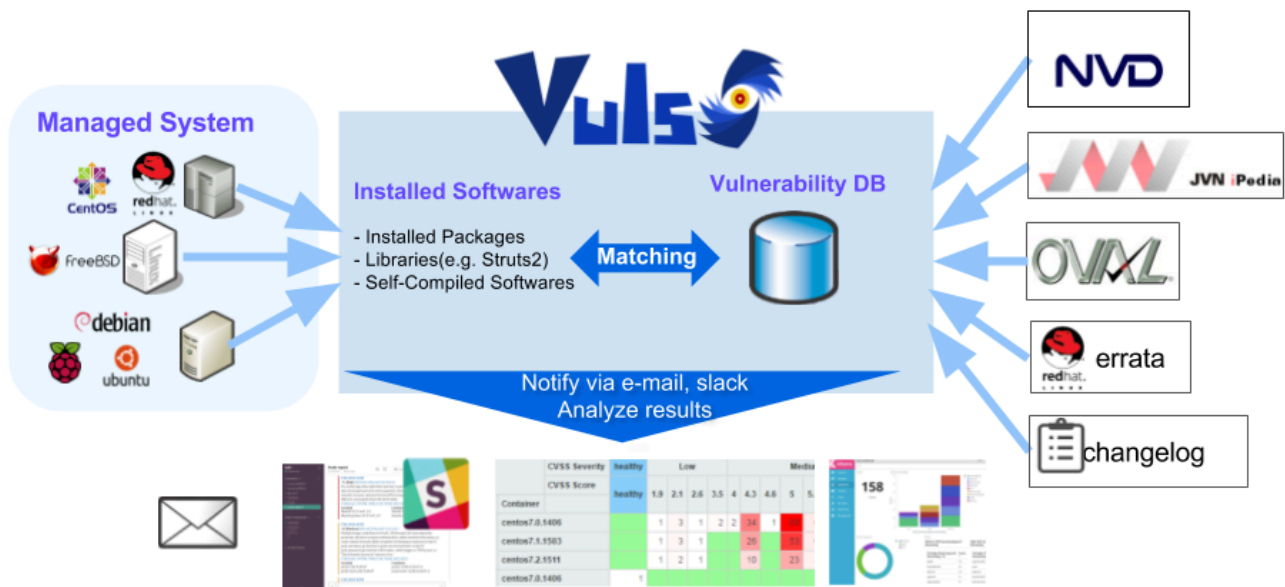
Agentless Vulnerability Scanner for Linux/FreeBSD

TUTORIAL

SUPPORTED OS

GITHUB

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





Run Anyware

Cloud, on-premise, Docker and supports major distributions.



High Quality Scan

Vuls uses multiple vulnerability databases NVD, JVN, OVAL, RHSA/ALAS/ELSA/FreeBSD-SA and Changelog.

Vuls v0.5.0 now possible to detect vulnerabilities that patches have not been published from distributors.



Remote and Local Scan

Remote scan mode is required to only setup one machine that is connected to other scan target servers via SSH. If you don't want the central Vuls server to connect to each server by SSH, you can use Vuls in the Local Scan mode.



Fast and Deep Scan

Fast scan mode scans without root privilege, no internet access, almost no load on the scan target server.
Deep scan mode scans in more detail.



Dynamic Analysis

It is possible to acquire the state of the server executing some commands. **Vuls v0.5.0** warns **not-restarting-processes which updated before but not restarting yet**. And detect processes affecting software update in advance.



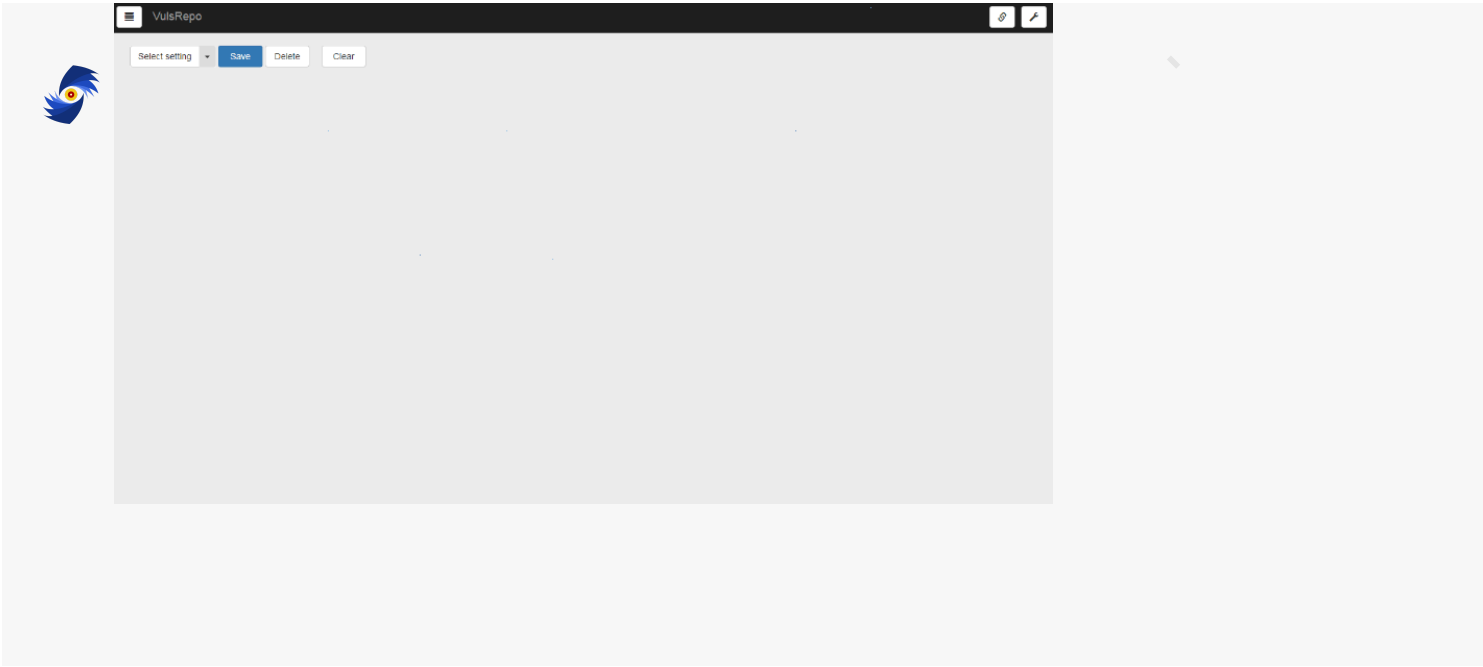
Scan Vulnerabilities of non-OS packages

It is possible to detect vulnerabilities in non-OS packages, such as something you compiled by yourself, language libraries and frameworks, that have been registered in the [CPE](#).

VulsRepo

VulsRepo is awesome OSS Web UI for Vuls. With VulsRepo you can analyze the scan results like Excel's pivot table. Demo is available

<https://usiusi360.github.io/vulsrepo/>



```
172.31.4.82 [ 1] CVE-2016-0799 | 10.0(High) | The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and
[ 2] CVE-2016-0483 | 10.0(High) | Unspecified vulnerability in the Java SE, Java SE Embedded, and JRockit compon
[ 3] CVE-2016-0494 | 10.0(High) | Unspecified vulnerability in the Java SE and Java SE Embedded components in Or
[ 4] CVE-2016-0705 | 10.0(High) | Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_am
[ 5] CVE-2016-0728 | 7.2 (High) | The join session keyring function in security/keys/process_keys.c in the Linux
[ 6] CVE-2016-1950 | 6.8 (Medium) | Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3
[ 7] CVE-2016-0778 | 6.5 (Medium) | The (1) roaming_read and (2) roaming_write functions in roaming_common.c in th

CVE-2016-1950
=====
CVSS Score
-----
6.8 (Medium) (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Summary
-----
Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x bef
ore 3.21.1, as used in Mozilla Firefox 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to
execute arbitrary code via crafted ASN.1 data in an X.509 certificate.

Package/CPE
-----
* nss-util-3.19.1-3.45.amzn1 -> nss-util-3.19.1-9.49.amzn1

Links
-----
* [NVD]( https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1950 )
* [MITRE]( https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1950 )
* [CveDetails]( http://www.cvedetails.com/cve/CVE-2016-1950 )
* [CVSSv2 Calculator]( https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2016-1950&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:P) )
* [RHEL-CVE]( https://access.redhat.com/security/cve/CVE-2016-1950 )
* [ALAS-2016-667]( https://alas.aws.amazon.com/ALAS-2016-667.html )
```

Terminal Based Viewer

Vuls has Terminal Based Viewer. You can view the scan result with vim-like keybindings.

Vuls
Docs Community Blog

Notification

Email and Slack notification is possible (supports Japanese language)

#vuls-report
2 members | Add a topic

CHANNELS (6)

- # centos20052
- # centos20062
- # general
- # random
- # trello
- #vuls-report**

DIRECT MESSAGES (4)

- slackbot

+ Invite People

CVE-2015-5312
7.1 (High) (AV:N/AC:M/Au:N/C:N/I:N/A:C)
The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.
[CVEDetails](#) / [MITRE](#) / [RHEL-CVE](#) / [RHSA-2015:2550](#)

Installed	Candidate
libxml2-2.9.1-5.el7_1.2	libxml2-2.9.1-6.el7_2.2
libxml2-python-2.9.1-5.el7_1.2	libxml2-python-2.9.1-6.el7_2.2

CVE-2015-8370
6.9 (Medium) (AV:L/AC:M/Au:N/C:C/I:C/A:C)
Multiple integer underflows in Grub2 1.98 through 2.02 allow physically proximate attackers to bypass authentication, obtain sensitive information, or cause a denial of service (disk corruption) via backspace characters in the (1) grub_username_get function in grub-core/normal/auth.c or the (2) grub_password_get function in lib/crypto.c, which trigger an "Off-by-two" or "Out of bounds overwrite" memory error.
[CVEDetails](#) / [MITRE](#) / [RHEL-CVE](#) / [RHSA-2015:2623](#)

Installed	Candidate
grub2-2.02-0.29.el7	grub2-1:2.02-0.34.el7_2
grub2-tools-2.02-0.29.el7	grub2-tools-1:2.02-0.34.el7_2

CVE-2015-8704

Who's Using This?

This project is used by all these people

FUTURE

sansan

iti
group

prott

IDCFrontier

SAKURA
internet

SmartHR

VELC



SEPTENIXGATE

DMM.com

Lancers

mazrica

LIVESENSE

MORE VULS USERS



Docs

Introduction

Architecture

Tutorial

Community

Join Slack

Slack

Twitter(English)

Twitter(Japanese)

More

Blog

GitHub



Copyright © 2018 kotakanbe