

Schwachstellenscans für Einrichtungen

SERVICEBESCHREIBUNG

Das LUIS führt Schwachstellenscans von zu der LUH gehörenden Systemen / Netzbereichen durch. Die genauen Parameter können bei Interesse besprochen und präzisiert werden. Eine Abstimmung mit den zuständigen **IT-Beauftragten** wird vorausgesetzt, idealerweise erfolgt die Kommunikation direkt mit den zuständigen IT-Beauftragten. Bei Interesse melden Sie sich gerne, schreiben Sie dazu eine **kryptographisch signierte** Mail an uns, geben Sie dazu folgende Daten an:

An: security@luis.uni-hannover.de

Betreff: Schwachstellenscans

Systeme / IP-Adressbereiche:

Ziel / Wünsche:

<https://www.luis.uni-hannover.de/de/services/it-sicherheit/schwachstellenscans>

Schwachstellenscans für Einrichtungen

- Worum geht es?
- Technische Beschreibung
- Ablauf
- Ergebnisse
 - 3 Beispiele
- Fragerunde

Worum geht es?

- Sicherheitslücken finden, Kriminellen zuvorkommen
- Awareness schaffen
- Netzwerkbasierte Angriffe/Scans
 - Keine lokalen Schwachstellen, die z. B. veraltetes (MS-/Libre-)Office erkennen könnten.
 - Nur für den OpenVAS/Greenbone-Host erreichbare Dienste.
- Bessere Informationen für Administrierende

Technische Beschreibung

- OpenVAS/Greenbone Community Feed
- Scanner klopft eine mögliche Sicherheitslücke nach der anderen ab und erstellt Liste
 - PDF und CSV
- Dauert Stunden bis mehrere Tage
- Viel Netzwerkverkehr/Logdaten auf den Geräten



Greenbone



Logos der eingesetzten Produkte, von <https://www.greenbone.net/en/feed-comparison/>
(aufgerufen am 02.05.2024)

Ablauf

- Institut meldet sich bei uns:
 - IT-Beauftragte*r mit S/MIME-signierter Mail.
- Wir vereinbaren Startzeit und Netzbereich(e).
- Vorbereitung beim Institut:
 - Evtl. Vorübergehende Freischaltungen in lokalen Firewalls für die mitgeteilte Scanner-IP.
 - Information an Administrierende, da Scansystem IDS/IPS in Alarmbereitschaft setzen kann.
- Verschlüsselter (Mail & S/MIME) Versand der Ergebnisse (.pdf & .csv) an IT-Beauftragten.
- Institut nutzt Erkenntnisse und fragt ggf. bei Unklarheiten nach.

Ergebnisse

- Nur mittlere bis schwere Funde.
- QOD (Quality of Detection) zwischen 70% und 100%
 - Scanner kann sich irren.
- Tabellarische Übersicht pro Netzwerk sowie pro IP-Adresse.
- Sicherheit im Gesamtkontext verstehen:
 - Priorisieren
 - Nicht jeder Fund muss ein Problem darstellen.
 - Nicht jedes Problem/jede Schwachstelle wird gefunden.



Ergebnisse mit leichten bis schweren Funden und QOD>0%
(Symbolbild)

Beispiel 1

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

cpe:/o:debian:debian_linux:9

Detected by OS Detection Consolidation and Reporting (OID:
↔.105937)

...continues on next page ...

2 RESULTS PER HOST

3

... continued from previous page ...

Summary

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection: 80

Vulnerability Detection Result

The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:9

Installed version,

build or SP: 9

EOL date: 2022-06-30

EOL info: [https://en.wikipedia.org/wiki/List_of_Debian_releases#Release
↔_table](https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table)

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security



Beispiel 1

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.
Quality of Detection: 80
Vulnerability Detection Result The "Debian GNU/Linux" Operating System on the remote host has reached the end of life. CPE: cpe:/o:debian:debian_linux:9 Installed version, build or SP: 9 EOL date: 2022-06-30 EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_history_table
Impact An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Solution: Solution type: Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
Vulnerability Detection Method Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID: Version used: 2022-04-05T13:00:52Z
Product Detection Result Product: cpe:/o:debian:debian_linux:9 Method: OS Detection Consolidation and Reporting OID:



2.3.1 Medium 443/tcp

Beispiel 2

Medium (CVSS: 5.0)
NVT: Missing 'Secure' Cookie Attribute (HTTP)
Summary
... continues on next page ...

2 RESULTS PER HOST

21

...continued from previous page ...
The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.
Quality of Detection: 80
Vulnerability Detection Result The cookies: Set-Cookie: sid=***replaced***; path=/ Set-Cookie: sid=***replaced***; path=/ are missing the "Secure" cookie attribute.
Solution: Solution type: Mitigation - Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection - Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)



2.5.1 Medium 636/tcp

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Quality of Detection: 98

Vulnerability Detection Result

In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.5.5.7.1.3) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

...continues on next page ...



Beispiel 3

... continued from previous page ...

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight

The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:

- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method

Check the used SSL protocols of the services provided by this system.

Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

OID:

Version used: 2021-10-15T12:51:02Z

References

cve: CVE-2016-0800

cve: CVE-2014-3566

url: <https://ssl-config.mozilla.org/>

url: <https://bettercrypto.org/>

url: <https://drownattack.com/>

url: <https://www.imperialviolet.org/2014/10/14/poodle.html>



Frage: Fragen?



Quellenangaben

- Screenshot Seite 1:
<https://www.luis.uni-hannover.de/de/services/it-sicherheit/schwachstellenscans> aufgerufen am 02.05.2024
- Logos Seite 4: <https://www.greenbone.net/en/feed-comparison/> (aufgerufen am 02.05.2024)
- Screenshots der Beispiele S. 7-11: PDF-Ergebnisse von OpenVAS/Greenbone-Scans.
- Bücherstapel (S.6), Fragezeichen-im-Rahmen (S.12) und Lese-Fuchs (S.7-11): <https://emojikitchen.dev/> aufgerufen am 02.05.2024
- Präsentationsvorlage: <https://www.intern.luis.uni-hannover.de/de/vorlagenformulare/layout-vorlagenformulare> aufgerufen am 02.05.2024