My Scans

Import   New Folder   ⊕ New Scan

This folder is empty. Create a new scan.

Tenable News

Siemens Automation License Manager almsrv64x.exe i...

Read More

«

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

TENABLE

Community

Research

Plugin Release Notes

Tenable News

CVE-2021-20123, CVE-2021-20124: DrayTek Vulnerabil...

Read More

VULNERABILITIES

Basic Network Scan	Advanced Scan	Advanced Dynamic Scan	Malware Scan	Mobile Device Scan
A full system scan suitable for any host.	Configure a scan without using any recommendations.	Configure a dynamic plugin scan without recommendations.	Scan for malware on Windows and Unix systems.	Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests	Credentialed Patch Audit	Active Directory Starter Scan	Find AI
Scan for published and unknown web vulnerabilities using Nessus Scanner.	Authenticate to hosts and enumerate missing updates.	Look for misconfigurations in Active Directory.	AI, LLM, ML related detections and vulnerabilities

COMPLIANCE

Audit Cloud Infrastructure	Internal PCI Network Scan	MDM Config Audit	Offline Config Audit	PCI Quarterly External Scan
Audit the configuration of third-party cloud services.	Perform an internal PCI DSS (11.2.1) vulnerability scan.	Audit the configuration of mobile device managers.	Audit the configuration of network devices.	Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing	SCAP and OVAL Auditing
Audit system configurations against a known baseline.	Audit systems using SCAP and OVAL definitions.

FOLDERS
- 📁 My Scans
- 📁 All Scans
- 🗑 Trash

RESOURCES
- ⭐ Policies
- 🔌 Plugin Rules
- 🐍 Terrascan

New Scan / Basic Network Scan
‹ Back to Scan Templates

Settings   Credentials   Plugins 👁

BASIC ⌄
- ● General
- Schedule
- Notifications

DISCOVERY ›
ASSESSMENT ›
REPORT ›
ADVANCED ›

Name	my first scan
Description	
Folder	My Scans ▼
Targets	172.31.98.11
Upload Targets	Add File

Save ▼   Cancel

FOLDERS

📂 My Scans

🗄 All Scans

🗑 Trash

RESOURCES

✪ Policies

🔲 Plugin Rules

👁 Terrascan

My Scans

Import   New Folder   ➕ New Scan

	Name	Scan Type	Schedule	Last Scanned ▾		
☐	my first scan	Vulnerability	On Demand	📅 N/A	►	✕

Search Scans 🔍   **1** Scan

Launch

FOLDERS

- 📂 My Scans
- 📁 All Scans
- 🗑 Trash

RESOURCES

- ✪ Policies
- ⊚ Plugin Rules
- ⊚ Terrascan

My Scans

Import   New Folder   ⊕ New Scan

Search Scans 🔍   **1** Scan

	Name	Scan Type	Schedule		Last Scanned ▾		
☐	my first scan	Vulnerability	On Demand	✓	Today at 1:55 AM	▶	✕

Tenable News

Cybersecurity Snapshot: RansomHub Group Triggers C...

Read More

FOLDERS
- 📁 My Scans
- 📁 All Scans
- 🗑 Trash

RESOURCES
- 🛡 Policies
- 😈 Plugin Rules
- 🌀 Terrascan

my first scan
‹ Back to My Scans

Configure   Audit Trail   Launch ▼   Report   Export ▼

Hosts 1	Vulnerabilities 26	History 1

Filter ▼   Search Hosts 🔍   1 Host

	Host	Vulnerabilities ▾
☐	172.31.98.11	11 · 76 ✕

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v2.0 ✎
Scanner:	Local Scanner
Start:	Today at 1:50 AM
End:	Today at 1:55 AM
Elapsed:	5 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

«

Vulnerabilities   26

MEDIUM   SSL Certificate Signed Using Weak Hashing Algorithm   ‹ ›

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

See Also

https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

Output

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject           : CN=DESKTOP-K0E0N56
Signature Algorithm : SHA-1 With RSA Encryption
Valid From        : May 19 19:05:13 2024 GMT
Valid To          : Nov 18 19:05:13 2024 GMT
Raw PEM certificate :
    BEGIN CERTIFICATE
more...
```

To see debug logs, please visit individual host

Port ▴	Hosts
3389 / tcp / msrdp	172.31.98.11 ✎

Plugin Details

Severity:	Medium
ID:	35291
Version:	1.33
Type:	remote
Family:	General
Published:	January 5, 2009
Modified:	December 15, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 3.4
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.2
Exploit Prediction Scoring System (EPSS): 0.0111
Risk Factor: Medium
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:P/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.7
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.9
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector:
CVSS2#E:POC/RL:OF/RC:C

Vulnerability Information