There's an error with your feed. Click here to view your license information.

Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Networkscan_Policy / Plugin #104743

‹ Back to Vulnerability Group

Vulnerabilities 14

MEDIUM

TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Output

```
TLSv1 is enabled and the server supports at least one cipher.
```

Port ▲	Hosts
2087 / tcp / www	paramountassure.com
443 / tcp / www	paramountassure.com
8443 / tcp / www	paramountassure.com
2083 / tcp / www	paramountassure.com
2053 / tcp / www	paramountassure.com
2096 / tcp / www	paramountassure.com

Plugin Details

Severity:	Medium
ID:	104743
Version:	1.9
Type:	remote
Family:	Service de
Published:	Novembe
Modified:	March 31,

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:H/PR:N/U

CVSS v2.0 Base Score: 6.1

CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:(

Vulnerability Informatio

Asset Inventory: True

Tenable News

Google Cloud Platform (GCP) Privilege Escalation V...

Read More

«