❗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 #157288

‹ Back to Vulnerability Group

Vulnerabilities 14

MEDIUM

TLS Version 1.1 Protocol Deprecated

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

See Also

https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d

Output

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

Port ▲	Hosts
2087 / tcp / www	paramountassure.com
443 / tcp / www	paramountassure.com
8010 / 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:	157288
Version:	1.2
Type:	remote
Family:	Service de
Published:	April 4, 20
Modified:	April 11, 2

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

Multiple Vulnerabilities in Adobe FrameMaker Publi...

Read More

«