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 #42873

‹ Back to Vulnerability Group

Vulnerabilities 14

HIGH

SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     ----------
-----------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-
CBC(168)          SHA1

more...
```

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:	High
ID:	42873
Version:	1.21
Type:	remote
Family:	General
Published:	Novembe
Modified:	February

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

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

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P

Vulnerability Informatio

Vulnerability Pub Date: Aug

In the news: true

Reference Information

CVE: CVE-2016-2183

Tenable News

Google Cloud Platform Remote Code Execution Vulner...

Read More