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 #51192

‹ Back to Vulnerability Group

Vulnerabilities 14

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=FG6H0ETB21903185/E=support@fortinet.com
|-Issuer  : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=FG6H0ETB21903185/E=support@fortinet.com
```

Port ▲	Hosts
8010 / tcp / www	paramountassure.com

Plugin Details

Severity:	Medium
ID:	51192
Version:	1.19
Type:	remote
Family:	General
Published:	Decembe
Modified:	April 27, 2

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

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

CVSS v2.0 Base Score: 6.4

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

Tenable News

Cybersecurity Snapshot: U.K. Cyber Agency Urges So...

Read More