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 #57582

Back to Vulnerability Group

Vulnerabilities 14

MEDIUM SSL Self-Signed Certificate

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Output

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : 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:	57582
Version:	1.5
Type:	remote
Family:	General
Published:	January 1
Modified:	April 27, 2

Risk Information

Risk Factor: Medium

CVSS v2.0 Base Score: 6.4

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

Tenable News

Microsoft's June 2024 Patch Tuesday Addresses 49 C...

Read More