


Remediation Tickets

How to Create Tickets

To create and assign a ticket in the top navigation bar, click **Vulnerability Management > Reports** and select a report.

Reports 1 of 1

Reports by Severity Class (Total: 1)



Date ▼	Status	Scan
Tue, Jul 23, 2019 6:52 PM UTC	Completed	Ubuntu

A blue arrow points from the 'Date' column header to the date 'Tue, Jul 23, 2019 6:52 PM UTC' in the table below the chart.

Tip

You can access the vulnerabilities from the **Vulnerability Scanning > Scans**.

The Results page will show up and you can click on the vulnerability:

Information	Results (25 of 27)	Hosts (1 of 1)	Ports (3 of 3)	Applications (1 of 1)	Operating Systems (1 of 1)	Open CVEs (1 of 1)	Proactively Closed (0 of 0)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
Vulnerability Severity										
CPE Inventory 0.0 Log										
Hostname Determination Reporting 0.0 Log										
CGI Scanning Consolidation 0.0 Log										
CGI Scanning Consolidation 0.0 Log										
SSH Protocol Versions Supported 0.0 Log										
HTTP Security Headers Detection 0.0 Log										
HTTP Security Headers Detection 0.0 Log										
OpenSSH Detection Consolidation 0.0 Log										
SSH Protocol Algorithms Supported 0.0 Log										
Traceroute 0.0 Log										
SSL/TLS: HTTP Public Key Pinning (HPKP) Missing 0.0 Log										
SSL/TLS: HTTP Strict Transport Security (HSTS) Missing 0.0 Log										
SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing 0.0 Log										
SSL/TLS: Report Medium Cipher Suites 0.0 Log										
SSL/TLS: Report Non Weak Cipher Suites 0.0 Log										
SSL/TLS: Report Supported Cipher Suites 0.0 Log										
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS 5.0 Medium										
OS Detection Consolidation and Reporting 0.0 Log										
No 404 check 0.0 Log										
SSL/TLS: Collect and Report Certificate Details 0.0 Log										
SSH Server type and version 0.0 Log										
Services 0.0 Log										
Services 0.0 Log										
Services 0.0 Log										
Services 0.0 Log										

The **Details** window appears. From there, you can select the vulnerability that you want to open a ticket for:

SSL/TLS: Report Supported Cipher Suites

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

0.0 Log

5.0 Medium

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exist only on HTTPS services.

Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method

Details: [SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID: 1.3.6.1.4.1.25623.1.0.108031](#)

Version used: 2017-02-08T07:56:44-04:00

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Solution

Solution Type: ↗ Mitigation
 The configuration of these services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

References

CVE [CVE-2016-2183](#)
[CVE-2016-6329](#)

OS Detection Consolidation and Reporting

No 404 check

0.0 Log

0.0 Log

The **Vulnerability** window appears. From there, you can click on the button **Create Ticket**:

Mageni Security

Dashboards Vulnerability Scanning Vulnerability Management Assets Management

Result: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

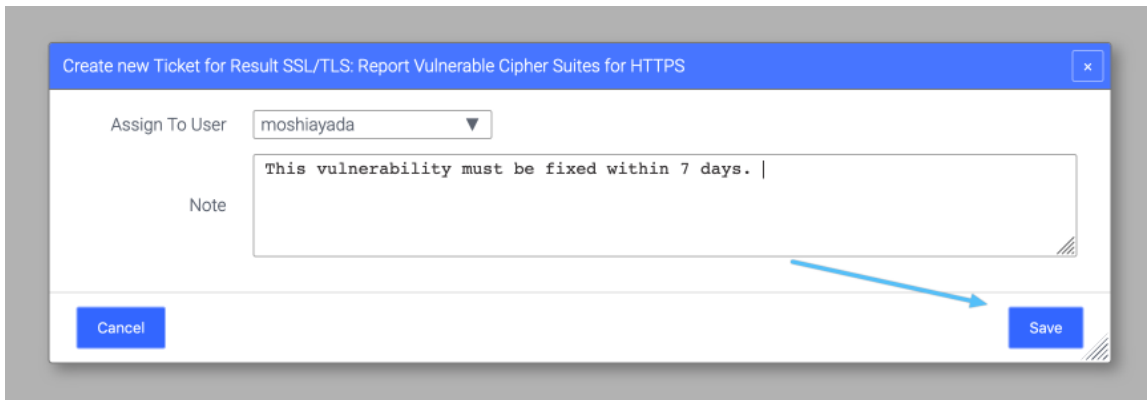
Information User Tags (0)

Vulnerability

Name SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Severity **5.0 Medium**

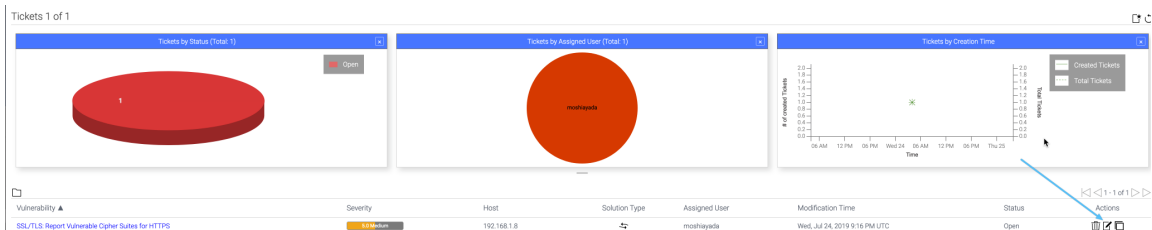
The **Create New Ticket** window appears. Now you can assign the ticket to an user and add a comment. Click on the **Save** button to save the new ticket:



Remediation Ticket Dashboard

Dashboard

In the top navigation bar, click **Vulnerability Management > Remediation Tickets**. The Dashboard page will show up and you can click on **Edit Ticket** button to edit the ticket:



The **Edit Ticket** window appears. There you can change the status of the ticket from Open to Fixed or Closed.

Open

Edit Ticket SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Status

Assigned User

Note for Open

Note for Fixed

Note for Closed

Cancel Save

Understanding the Terms

? New Scan Window

1. **Open:** It is a ticket whose vulnerability has not been fixed or closed.
2. **Fixed:** You fixed the vulnerability.
3. **Closed:** The vulnerability was closed.
4. **Notes for Open:** Notes that you can create when you open a ticket.
5. **Notes for Fixed:** Notes that you can create when the ticket have been fixed.
6. **Notes for Closed:** Notes that you can create when the ticket have been closed.