QualityNet | Security

**November 27, 2023**

# Update: QualityNet Tenable Vulnerability for libcurl: Extension Approved

This notice is an update to the previous communication on this topic sent on Thursday, November 16, 2023. The Centers for Medicare & Medicaid Services (CMS) has approved an additional extension for this issue until further notice. CMS Security will continue working with Cloud Operations and Maintenance (CCOM) and Enterprise Shared Services (ESS) to track the issue with the various vendors. Application Development Organizations (ADOs) do not have any action at this time. Any additional information or notices will be communicated via Slack, the Bi-weekly DevSecOps, and/or Bi-weekly Security meetings.

Due to the TrendMicro agents installed throughout various hosts within the QualityNet Environment, Nessus has detected a Critical finding affecting all hosts running the agents, which is being reflected on ADO Vulnerability reports. CMS has approved an Enterprise-wide Extension regarding Nessus findings related to libcurl listed below:

**Impacted Tenable Nessus Plugin(s)**
182873 & 182874

**Affected Systems**

| System | Additional Information | Scanning Results |
|---|---|---|
| **TrendMicro (agents)** | TrendMicro has confirmed that Deep Security Manager and Agents are not affected by this vulnerability. In addition, this vulnerability is mitigated since the configuration in order to exploit the vulnerability is not enabled by default within CURL https://success.trendmicro.com/dcx/s/solution/000295396?language=en_US | When scanning, Tenable simply does a version check against the CURL libraries and binary version 8.4 and will continue to show in reporting. |
| **AWS Linux** | The latest curl-8.3.0-1 version available in the Amazon Linux repository is backported with patches. This means that a security fix for the CVEs has been applied to "8.3.0" version itself instead of releasing a new version altogether in case of Amazon Linux 2/2023. | When scanning, Tenable simply does a version check against the CURL libraries and binary version 8.4 and will continue to show in reporting. |

| | | |
|---|---|---|
| **RHEL** | **RHEL 8** - RedHat Support Case: 03654298. Per https://access.redhat.com/security/cve/cve-2023-38545 - this version of RHEL is not affected by the CVE. Per https://access.redhat.com/security/cve/cve-2023-38546 - this version of RHEL is affected and a fix is not available yet.<br><br>**RHEL7** - https://access.redhat.com/security/cve/cve-2023-38545 - this version of RHEL is not affected by the CVE. Per https://access.redhat.com/security/cve/cve-2023-38546 - this version of RHEL is out of support scope. | When scanning, Tenable simply does a version check against the CURL libraries and binary version 8.4 and will continue to show in reporting. |

Questions or concerns can be directed to your Information System Security Officer (ISSO), or the gnet-security-community Slack channel.

***If you need additional information, please work with your assigned CMS Information System Security Officer (ISSO): List here , the HIDS Security Analyst team, or reach out on QualityNet Slack: #qnet-security-community.***

***Join the QualityNet Mailer List:***
**Qnet Security Communications**