QualityNet | Security

November 16, 2023

QualityNet Tenable Vulnerability for libcurl: Extension Approved thru 11/27/2023

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 Application Development Organization (ADO) Vulnerability reports. The purpose of this notification is to inform the QualityNet ADOs that 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.	When scanning, Tenable simply does a version check against the CURL libraries and binary version 8.4 and will continue to show in reporting.

	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.	

Additional information will be communicated via Slack channels, the Bi-weekly DevSecOps meeting, and/or Bi-weekly Security meetings.

Questions or concerns can be directed to your Information System Security Officer (ISSO), or the qnet-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

Center for Clinical Standards and Quality (CCSQ)