Security Advisory

Published: January 2022

CVE-2021-44228, CVE-2021-45046, CVE-2021-4104

Marvell was made aware of vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-4104) associated with Apache Tomcat servers with Log4j that could potentially affect the following Marvell product applications:

- QCC GUI v5.5.00.85, and prior (EOS – no support)
- QCC vCenter Plug-In:
  - v2.0.33-4, and prior
  - v2.0.36-7, and prior
- Applicable to both QLogic® Fibre Channel and FastLinQ® Ethernet installations

Marvell places the highest priority on addressing security concerns. While Marvell believes that the above product applications are not affected by the referenced vulnerabilities, Marvell, out of an abundance of caution, has been working with its direct customers to provide recommended resolutions and updates.

Marvell encourages customers to contact their Marvell representative for any additional support.

Published: January 2021

CVE-2020-5804/CVE-2020-5805 (TRA-2020-56)

Marvell was made aware of two new vulnerabilities associated with the QConvergeConsole GUI (QCC GUI) in October 2020. These vulnerabilities were made public by Tenable in January 2021, and are posted here: https://www.tenable.com/security/research

Marvell is currently working towards a software release update, which replaces all previous versions of the software and resolves the above-mentioned vulnerability.

Marvell encourages customers to contact their Marvell representative for any additional support.

Published: December 2020

CVE-2020-5803 (TRA-2020-56)

Marvell was made aware of a new vulnerability associated with the QConvergeConsole GUI (QCC GUI) in September 2020. This vulnerability was made public by Tenable in December 2020, and is posted here: https://www.tenable.com/security/research

Marvell is currently working towards a software release update, which replaces all previous versions of the software and resolves the above-mentioned vulnerability.

Marvell encourages customers to contact their Marvell representative for any additional support.

Published: September 2020

CVE-2020-15643 (ZDI-CAN-10549) / CVE-2020-15644 (ZDI-CAN-10550) / CVE-2020-15645 (ZDI-CAN-10553)

Marvell was made aware of the partial fixes from Tenable in September 2020.

Marvell is currently working towards a software release update, which replaces all previous versions of the software and resolves the above-mentioned vulnerabilities.

Marvell encourages customers to contact their Marvell representative for any additional support.

Published: July 2020

ZDI-CAN-10496/10497/10499/10501/10502/10549/10550/10553/10565/10799

Marvell was made aware of vulnerabilities in the *Apache Tomcat Server* associated with the QConvergeConsole GUI (QCC GUI) management application. These vulnerabilities were made public by ZDI in April 2020, and are posted here: https://www.zerodayinitiative.com/advisories/upcoming/.

Marvell places the highest priority on addressing security concerns. Once notified, Marvell immediately collaborated with ZDI to resolve the vulnerabilities, then worked with our direct customers to communicate these vulnerabilities and provide a new software release, QCC GUI v5.5.00.73.

This new release replaces all previous versions of the software and resolves the aforementioned vulnerabilities.

Marvell encourages customers to contact their Marvell representative for any additional support.