Reference: Apache Log4j Vulnerability, 12/14/2021, Update 1/6/2022

Issue:
The Apache Software Foundation has released a security advisory to address a remote code execution vulnerability (CVE-2021-44228) affecting Log4j versions 2.0-beta9 to 2.14.1. A remote attacker could exploit this vulnerability to take control of an affected system. Log4j is an open-source, Java-based logging utility widely used by enterprise applications and cloud services.

Response:
Comnet has identified a potential Apache Log4j vulnerability with customers that use the Maxview Storage Manager component to manage Microchip SmartRAID Controllers. This vulnerability log4j 2.14.0 is impacted in Maxview Storage Manager Version 3.10.2470 and below. Microchip has released a patched version that remediates this vulnerability.
Units that may be affected and should be patched:

- Razberi ServerSwitchIQ Appliance Models with 64bit Windows Operating Systems
  - SSIQ24P-2-XE-XXT
  - SSIQ24PU-2-XE-XXT
  - SSIQ24PX-2-XE-XXT
  - SSIQ24PX2U-2-XE-XXT

- Razberi Legacy Core Server Models with 64bit Windows Operating Systems
  - CP2
  - CE2

The Maxview Storage Manager patched version 4.01.24713 for Windows 64bit can be found at the following download links

- Razberi Support - msm_windows_x64_v4_01_24713.zip
- Microchip Support - msm_windows_x64_v4_01_24713.zip

Contact Information:
If you have any further questions, please contact your Comnet/Razberi sales representative or technical support representative.

Additional Information:
NVD - CVE-2021-44228 (nist.gov)