SALIENT

Technical Bulletin

Reference #: TB211201SU

Title: Apache Log4j Vulnerability
Date: December 16, 2021

Description:

On December 10, 2021, notice of a critical remote code vulnerability was published concerning the Apache Log4j library. Vulnerable versions include Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0. The vulnerability is specific to log4j-core and does not extend to log4net, log4cxx, or other Apache Logging Services. Bad actors may use log messages or log message parameters to execute arbitrary code on the targeted server. Salient Systems is in the process of assessing potential impact to its products. Follow the links in the following sections for more detailed information on the vulnerability.

Vulnerability ID:

CVE-2021-44228

Issue Summary:

Apache Publication: Apache Log4j Remote Code Execution
CVE Details: CVE-2021-44228

Vulnerable Products

Salient Model	Vendor	Vendor Model	Expected Patch	Vendor Reference
Power Pro-R	Dell	Dell Open Management Enterprise – Modular, DellEMC OpenManage Enterprise Services , OpenManage Enterprise	12/17/2021	Dell Response
Power Plus	Dell	Dell Open Management Enterprise – Modular, DellEMC OpenManage Enterprise Services , OpenManage Enterprise	12/17/2021	Dell Response
Power Ultra	Dell	Dell Open Management Enterprise – Modular, DellEMC OpenManage Enterprise Services , OpenManage Enterprise	12/17/2021	Dell Response
Power Platinum	Dell	Dell Open Management Enterprise – Modular, DellEMC OpenManage Enterprise Services , OpenManage Enterprise	12/17/2021	Dell Response
RM3000	Dell	Dell Open Management Enterprise – Modular, DellEMC OpenManage Enterprise Services , OpenManage Enterprise	12/17/2021	Dell Response

Other products under investigation:

Products containing the Broadcom MegaRAID LSI00214 RAID controller using the Broadcom MegaRAID Storage Manager

- RM1100
- RM2500
- RM2800

Unaffected Products:

- Salient CompleteView VMS
- Salient CompleteView web client
- Salient TouchView Mobile – Android
- Salient TouchView Mobile – IOS

Pending Resolution:

Any security updates or mitigations will be communicated at https://www.dell.com/support/security as soon as they become available.

Recommendations:

Customers are encouraged to follow security best practices including those recommended by Apache (Apache Log4j Remote Code Execution) and continue to monitor this notice and the vendor website (above) for further updates as they become available.