

Technical Support Bulletin

High-Risk Security Exposures in Apache Log4j Java Library



ALERT! Products that use the Apache Log4j Java library may be vulnerable to unauthorized remote code execution attacks and denial-of-service attacks.

Issue Summary

Computer systems exposed to the internet and running applications that use most 2.x.x versions of the Apache Log4j Java library are vulnerable to unauthorized remote code execution attacks. A remote LDAP server can take control of the system using a simple message string. This security issue has been assigned the Common Vulnerabilities and Exposures number CVE-2021-44228.

Log4j version 2.15.0 was released to address this issue. However, the fix was found to be incomplete, leaving Log4j vulnerable to denial-of-service attacks. This further vulnerability is identified as CVE-2021-45046.

Both issues are resolved in Log4j version 2.12.2 for Java 7 and 2.16.0 for Java 8 and higher. It remains for software vendors to incorporate the new libraries into their own products.

Developed by the Apache Software Foundation, Log4j is a widely used, open source Java library for logging error messages in application software. Vendors with products affected by the Log4j vulnerability include Amazon (AWS), Apache (Hadoop), Apple (iCloud), Atlassian, Cisco, Commvault, ESRI, Exact, Fortinet, IBM, JetBrains, Microsoft (Azure), Minecraft, Nelson, Nutanix, OpenMRS, Oracle, Red Hat, Splunk, Soft, and VMware.

The National Vulnerability Database (NVD) of the U.S. National Institute for Standards and Technology (NIST) rates the severity of CVE-2021-44228 at 10 out of 10. The severity of CVE-2021-45046 has not yet been rated.

Affected DDN Products

DDN Engineering has determined that no DDN At Scale products, as shipped from the factory, are affected by the Log4j issue.

However, DDN GRIDScaler may have been configured at the customer site to use IBM SKLM or the IBM Spectrum Scale GUI. Certain versions of both these options are known to be exposed to the Log4j security vulnerability.

ALERT! If your GRIDScaler configuration includes an SKLM or Spectrum Scale GUI option, please contact DDN Support immediately for problem determination and mitigation assistance.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or need assistance. Support can be reached online, by email, or by phone as listed below.

Web

DDN Community Support Portal <https://community.ddn.com/login>
Portal Assistance webportal.support@ddn.com

Email

Support Email support@ddn.com

Telephone

DDN Support Worldwide Directory <https://www.ddn.com/support/global-services-overview/>

Bulletins & Notices

Support Bulletins <http://www.ddn.com/support/technical-support-bulletins>
End-of-Life Notices <http://www.ddn.com/support/end-of-life-notices>
Release Notes <https://community.ddn.com/login>
Subscription Requests support-tsb@ddn.com