Oracle Security Alert Advisory - CVE-2021-44228

Description

This Security Alert addresses CVE-2021-44228, a remote code execution vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password.

Due to the severity of this vulnerability and the publication of exploit code on various sites, Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the product listed below. The product area is shown in the Patch Availability Document column.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Affected Products and Versions	Patch Availability Document
Apache Log4j, versions 2.0-2.14.1	My Oracle Support Document

Security Alert Supported Products and Versions

Patches released through the Security Alert program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Lifetime Support Policy. Oracle recommends that customers plan product upgrades to ensure that patches released through the Security Alert program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Security Alert. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in My Oracle Support Note 209768.1. Please review the Technical Support Policies for further guidelines regarding support policies and phases of support.

References

- Oracle Critical Patch Updates, Security Alerts and Bulletins
- Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions
- Risk Matrix Definitions
- Use of Common Vulnerability Scoring System (CVSS) by Oracle
- English text version of the risk matrices
- CVRF XML version of the risk matrices
- Map of CVE to Advisory/Alert
- Oracle Lifetime support Policy
- JEP 290 Reference Blocklist Filter

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly addressed by the patches associated with this advisory. Risk matrices for previous security patches can be found in previous Critical Patch Update advisories and Alerts. An English text version of the risk matrices provided in this document is here.

Security vulnerabilities are scored using CVSS version 3.1 (see Oracle CVSS Scoring for an explanation of how Oracle applies CVSS version 3.1).

Oracle conducts an analysis of each security vulnerability addressed by a Security Alert. Oracle does not disclose detailed information about this security analysis to customers, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see Oracle vulnerability disclosure policies.

Oracle lists updates that address vulnerabilities in third-party components that are not exploitable in the context of their inclusion in their respective Oracle product beneath the product's risk matrix.

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Security Alert to Oracle: None credited in this Security Alert.

Modification History

Date	Note
2021-December-10	Rev 1. Initial Release.

Third Party Component Risk Matrix

This Security Alert contains 1 new security patch for Third Party Component. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found here.

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (				
					Base Score	Attack Vector	Attack Complex	Privs Req'd	In
CVE-2021-44228	Apache Log4j	All	Multiple	Yes	10.0	Network	Low	None	N