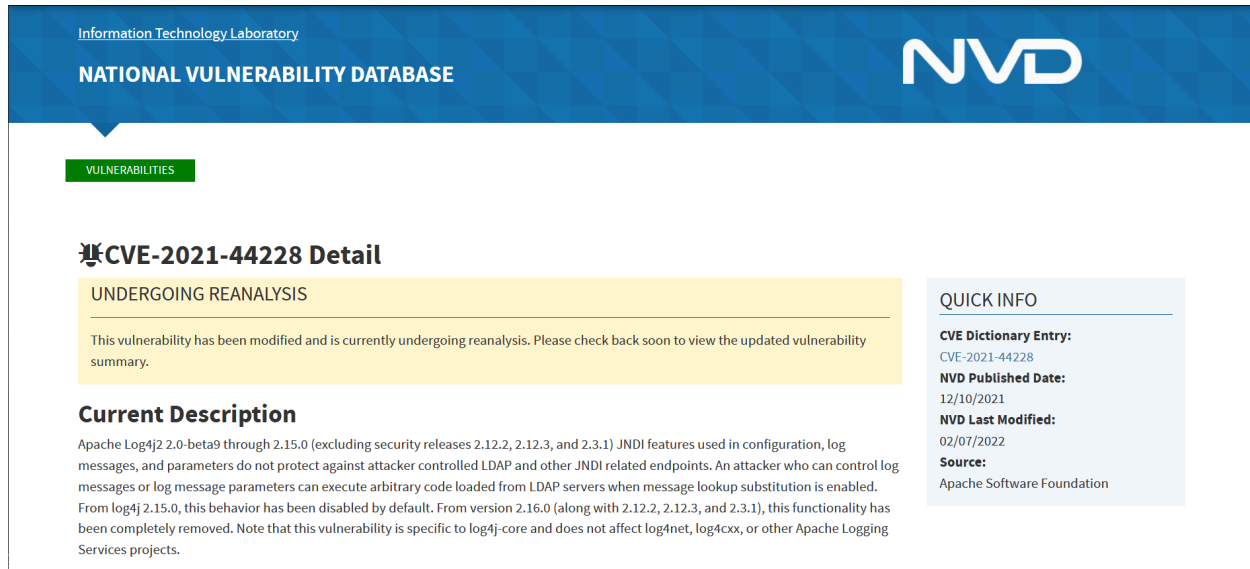


# Log4j exploit



Information Technology Laboratory  
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

## CVE-2021-44228 Detail

UNDERGOING REANALYSIS

This vulnerability has been modified and is currently undergoing reanalysis. Please check back soon to view the updated vulnerability summary.

### Current Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

#### QUICK INFO

**CVE Dictionary Entry:**  
CVE-2021-44228

**NVD Published Date:**  
12/10/2021

**NVD Last Modified:**  
02/07/2022

**Source:**  
Apache Software Foundation

Log4j vulnerability discovered on December 9, 2021. It is a java software library and widespread in other software and applications used worldwide. Log4j is estimated to be present in over 100 million instances globally. This vulnerability and associated attacks against it are being characterized as Log4Shell in the cybersecurity community. According to National Vulnerability Database (NVD) under the CVE-2021-44228 this vulnerability is rated 10 out of 10 which is critical.

Log4j allows users to specify custom code for formatting a log message and allows third-party servers to submit software code that can perform all kinds of actions on the targeted computer. For my understanding it is like SQL injection vulnerability but more simple and easier to exploit, due to being widely spread to all over the organizations.