CVE-2021-44228 Apache Log4j Vulnerabilities

CVE ID: CVE-2021-44228, CVE-2021-45046, CVE-2021-4104

First Published: December 21, 2021

Last Update: December 21, 2021

Status: Confirmed

Revision: 1

Overview

CVE was published cybersecurity experts have discovered an entirely new attack at the Apache Log4j2 release that could lead to information leaks, remote code execution (RCE) and local code execution (LCE) attacks.

In Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0, the JNDI Lookup features used in configurations, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. The flaw could be abused by an attacker to craft malicious input data using a JNDI Lookup function in a DoS attack.

Since Log4j 2.15.0, the behavior has been disable by default settings. From Log4j 2.16.0, this function has been completely removed.

NIST. December 10, 2021. CVE-2021-44228. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Affected Products

No **Vivitek Novo-series products** are affected by this vulnerability.

Workaround

None.

Solution

None.

Revision History

Revision 1 / December 21, 2021 / Initial release