

Pluribus Networks

CVE-2021-44228 (Apache Log4j2 utility) Vulnerability Notice



Copyright © 2021 Pluribus Networks All Rights reserved. The information contained herein is deemed to be accurate at the time of publication but is subject to change without notice and this information is provided on an “as is” basis and does not imply any kind of warranty. Netvisor is a registered trademark and Pluribus Networks, the Pluribus Logo and Freedom are trademarks of Pluribus Networks, Inc. Other product or service names may be trademarks or service marks of others.

CVE-2021-44228 (Apache Log4j2 utility) Vulnerability Notice

Problem Description

The Log4j vulnerability (CVE-2021-4428) is an unauthenticated, remote code execution (RCE) vulnerability that can lead to a system compromise. The vulnerability received a perfect CVSS score of 10, which illustrates the danger and seriousness of the exploit. Additionally, what can make the vulnerability more impactful than other security vulnerabilities is that CVE-2021-44228 can be used as a mechanism to deliver additional security exploits, thus making CVE-2021-44228 more than just a single vulnerability. The vulnerability is part of the Apache Java Log4j2 package, a common logging library used by many different applications and products.

Pluribus Engineering became aware of the vulnerability on December 9, 2021, and immediately started evaluating its impact on any Pluribus products.

In Apache log4j versions 2.0-beta9 to 2.14.1, 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.

Purpose of this document is to provide an update in response to the vulnerability and its exposure to Pluribus product and software.

Revision History

Revision	Date of Publish	Comments
1.0	December-13-2021	Initial Release
1.1	December-17-2021	Update for CVE-2021-4104 and UNUM release information

Please refer to the links below for an official explanation on this issue:

<https://logging.apache.org/log4j/2.x/security.html>

<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

Copyright © 2021 Pluribus Networks All Rights reserved. The information contained herein is deemed to be accurate at the time of publication but is subject to change without notice and this information is provided on an “as is” basis and does not imply any kind of warranty. Netvisor is a registered trademark and Pluribus Networks, the Pluribus Logo and Freedom are trademarks of Pluribus Networks, Inc. Other product or service names may be trademarks or service marks of others.

Affected Products

Following Pluribus Networks Product is affected by this vulnerability:

- **Pluribus UNUM Management Platform**

The UNUM platform was not using the offending Jndi Java class. The approach taken is to remove that java class from UNUM altogether. Upgrade for the UNUM platform is required to address the vulnerability.

Update: Pluribus Networks has posted the U620HF4 patch (build 6.2.0-8338) for the Pluribus UNUM Management Platform to the Pluribus Customer Portal to address the vulnerability.

Unaffected Products

Following Pluribus Networks Product is unaffected by this vulnerability:

- **Pluribus Netvisor ONE Operating System (nvOS)**

Pluribus Netvisor ONE Operating System (nvOS) is not vulnerable to log4j vulnerability tracked in CVE-2021-4428.

Update: Apache disclosed a new vulnerability (CVE-2021-4104) in log4j version that is in use by Netvisor. Although CVE-2021-4104 affects log4j version in use by Netvisor, it doesn't affect Netvisor as Netvisor doesn't use the JMSAppender in its log4j configurations.



Copyright © 2021 Pluribus Networks All Rights reserved. The information contained herein is deemed to be accurate at the time of publication but is subject to change without notice and this information is provided on an “as is” basis and does not imply any kind of warranty. Netvisor is a registered trademark and Pluribus Networks, the Pluribus Logo and Freedom are trademarks of Pluribus Networks, Inc. Other product or service names may be trademarks or service marks of others.