Apache log4j2 - Remote Code Execution (RCE)
December 2021

Advisory ID: nutanix-sa-023-log4j2

Last Updated: 04 January 2022
Published: 11 December 2021
Version: 1.15

Updates

CVE-2021-44832 (CVSSv3 of 6.6) requires an update to log4j v2.17.1. The attack vector and configurations required to exploit this CVE are not present in the current shipping product and pose a lower risk. At this time, we will be addressing this upgrade as part of our regular maintenance releases over the coming weeks. Please refer to Release Notes and the Nutanix Portal for more information as releases become available.

Please review the revision section at the end of this document for details on each change.

Summary

A critical vulnerability in Apache Log4j2 (CVE-2021-44228 and CVE-2021-45046) has been publicly disclosed that may allow for remote code execution in impacted Nutanix products.

Description

This issue only affects log4j versions between 2.0-beta9 and 2.15. The exploit requires an attacker to remotely access an endpoint and send arbitrary data logged or otherwise processed by the log4j engine.

On-prem products and services are at a slightly reduced risk so long as they are not positioned at the edge or in a way that could allow for an attacker to inject data into the logging engine. Trouble is by no means eliminated since attackers can and do gain access to internal protected networks at times. Once product updates are made available, they should be considered critical and updated immediately.

SaaS-based products, such as Nutanix Beam, Frame, Leap, and others, are under greater risk due to their internet-facing nature. Web endpoints are especially vulnerable since often strings such as User-Agent and Headers are logged by backend services. We have instituted Web Application Firewall (WAF) rules that filter attempts to exploit this vulnerability for all SaaS products. These instances are considered *mitigated* by the WAF but will be patched and updated in this advisory accordingly.

Tel: 1 (855) 688-2649 | **Fax:** 1 (408) 916-4039

The below table will now reflect mitigation and patching toward both CVE-2021-44228 and CVE-2021-45046 where appropriate. Patched or Mitigated status indicates coverage of both applicable CVEs. Products not impacted are not affected.

Nutanix Products

Product	Fix Release
AHV *(All supported versions)*	Not impacted
AOS (LTS – including Prism Element) AOS (STS – including Prism Element) AOS (Community Edition)	Not impacted Patched in 6.0.2.4, available on the Portal for download Not impacted
Calm *(All supported versions)*	Not impacted
Calm Tunnel VM *(All supported versions)*	Not impacted
Collector *(All supported versions)*	Not impacted
Era *(All supported versions)*	Not impacted
File Analytics *(Version 3.0+)* File Analytics *(Version 2.1.x, 2.2.x)*	Mitigated in version 3.0.1 which is available on the Portal for download Mitigation is available. Please reference https://portal.nutanix.com/kb/12499
Files *(All supported versions)*	Not impacted
Flow *(All supported versions)*	Not impacted
Foundation *(All supported versions)*	Not impacted
FSCVM *(All supported versions)*	Not impacted
Karbon *(All supported versions)*	Mitigation is available. Please reference *https://portal.nutanix.com/kb/12483*
LCM *(All supported versions)*	Not impacted
Mine *(All supported versions)*	Mitigation is available. Please reference *https://portal.nutanix.com/kb/12484*
Move *(All supported versions)*	Not impacted
MSP *(All supported versions)*	Mitigation is available. Please reference *https://portal.nutanix.com/kb/12482*
NCC *(All supported versions)*	Not impacted
NGT *(All supported versions)*	Not impacted
Objects *(All supported versions)*	Mitigation is available. Please reference *https://portal.nutanix.com/kb/12482*
Prism Central *(All supported versions)*	Patched in 2021-9.0.3 or higher, available on the Portal for download.
Volumes *(All supported versions)*	Not impacted
Witness VM *(All supported versions)*	Mitigation is available. Please reference https://portal.nutanix.com/kb/12491
X-Ray *(All supported versions)*	Not impacted

Tel: 1 (855) 688-2649 | **Fax:** 1 (408) 916-4039

The table below will now reflect mitigation and patching toward CVE-2021-44228 and CVE-2021-45046 where appropriate. Patched or Mitigated status indicates coverage of both applicable CVEs.

SaaS-Based Products with Web Application Firewall Protections

Product	Fix Release	WAF
Beam	Patched	Yes
BeamGov	Patched	Yes
Calm	Pending PC 2021.9.0.3 or higher upgrade	Yes
Collector Portal	Patched	Yes
Data Lens	Not impacted	Yes
Flow Security Central	Patched	Yes
Frame	Patched	Yes
FrameGov	Patched	Yes
Insights	Not impacted	Yes
Karbon Platform Service	Patched	Yes
Leap	Pending PC 2021.9.0.3 or higher upgrade	Yes
Sizer	Patched	Yes

Supported Versions

The following links describe our detailed Software End of Life Policies.

- Prism Central: https://download.nutanix.com/misc/PC_EOL/PC_EOL.pdf
- AOS: https://download.nutanix.com/misc/AOS_EOL/AOS_EOL.pdf
- Files: https://download.nutanix.com/misc/FILES_EOL/FILES_EOL.pdf
- General EOL Policy: https://www.nutanix.com/support-services/product-support/support-policies-and-faqs?show=accordion-0

Mitigations

Web Application Firewall (WAF) filters have been put into place for all Nutanix SaaS-based products. WAF rules provide temporary protection until proper product updates can be made available. These filters are adjusted multiple times per day to account for new and emerging vectors.

On-prem products, unless otherwise indicated, have no mitigations that are customer configurable. This document will be updated with the appropriate instructions or Knowledge Base (KB) articles if reliefs become available.

References

CISA - https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce
Apache - https://logging.apache.org/log4j/2.x/security.html

Tel: 1 (855) 688-2649 | **Fax:** 1 (408) 916-4039

Elastic Search - https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

If you have questions, please open a case with Nutanix Support or call Support at the phone numbers on the website https://www.nutanix.com/support-phone-numbers.

Thank you for being a Nutanix customer.

Revision History

Version	Section	Date
1.0	-	11 December 2021
1.1	Addition of Prism Central	11 December 2021
1.2	Sizer Patched in Production	12 December 2021
1.3	Update schedule, updated confirmations on AOS, PC and Volumes	12 December 2021 @ 9:00 PM PST
1.4	No impact added for AOS (LTS), AHV, Move, NCC, X-RAY, LCM, Era, Data Lens Patch status updated for Frame due to an error, FrameGOV and AOS (STS) Added on-prem versions of Calm, Karbon, File Analytics and MSP Adjusted date for revision 1.3.	13 December 2021 @ 3:00 PM PST
1.5	Flipped Flow and Flow Security Central into their proper categories. No impact added for Flow	13 December 2021 @ 7:00 PM PST
1.6	No impact added for Calm (SaaS), Insights, Era Change in status for Insights (SaaS). No impact determined. Updated patched status for Flow Security Central Added Community Edition and End of Life and Support Policy links.	14 December 2021 @ 11:30 AM PST
1.7	Patch status updated for File Analytics, Karbon, Beam, BeamGOV Change in status for Calm. No impact determined. Mitigations forthcoming for Objects, MSP, Mine	14 December 2021 @ 8:00 PM PST
1.8	Fixed Calm (SaaS) as incorrectly marked as not impacted. It is awaiting the PC upgrade. Adjusted language to make it clearer what's released and pending release. Alphabetized the lists for sanity. No impact added for Collector, and patched for Collector Portal	15 December 2021 @ 8:30 PM PST
1.9	No impact added for FSCVM, Calm – Tunnel VM Fixed PDF link issue	16 December 2021 @ 9:00 AM PST

1.10	Minor wording fixes Mitigation for Witness VM added. No impact added for NGT	16 December 2021 @ 10:30 AM PST
1.11	Addition of CVE-2021-45046 tracking Release of FA 3.0.1 Mitigation of earlier versions of FA forthcoming.	17 December 2021 @ 12:00 PM PST
1.12	Karbon Platform Services verified Mitigation script for FA versions prior to 3.0 PC (2021-9.0.3) is patched and available on the portal.	20 December 2021 @ 7:00 AM PST
1.13	AOS STS (6.0.2.4) is patched and available on the portal.	20 December 2021 @ 10:30 AM PST
1.14	Added version clarification for Prism Central upgrades.	4 January 2022 @ 11:00 AM PST
1.15	Added update for CVE-2021-44832	4 January 2022 @ 12:00 PM PST

Tel: 1 (855) 688-2649 | **Fax:** 1 (408) 916-4039