Security Advisory Report - OBSO-2112-01

Critical vulnerability in Apache Log4j (Log4Shell, CVE-2021-44228)

Release Date:	2021-12-13 18:42:27
Last Update:	2021-12-14 21:29:36

Summary

Apache Log4j2 <= 2.14.1 has a JNDI feature that allows it to look up the contents of a log message by using a name, via the LDAP protocol. Unfortunately though, it doesn't protect against attacker-controlled LDAP endpoints, which means that if an attacker can control log messages (or log message parameters) they can trigger a lookup to a malicious LDAP server, and subsequent loading and execution of arbitrary Java code.

The vulnerability is rated critical with an initial CVSS3 score of 10.(NVD has not been assigned a score yet)

Details

Key Takeaways

- Vulnerability is present in all applications embedding Log4j (ver. 2.0 to 2.14.1.) for audit logging feature. Mainly Apache stack but also applications like Elastic search, Redis, etc.
- Vulnerability based on forcing applications to log a specific string which forces vulnerable system to download and run malicious script from attacker-controlled domain.
- According to security researchers' apps and services across the globe has already been actively scanned for vulnerable versions of Log4j by malicious actors.
- Attack can be blocked with a config change and patch.
- Cisco Talos claims to observe threats such as Mirai attempting to leverage this vulnerability to automatically infect new systems.

Affected Products

Confirmed Affected products

Hipath DS-Win 4 R6.29.0 and higher (fixed in V4 R6.31.0 / available)
Atos Unify OpenScape UC V10.2.9.0 and higher (fix planned for V10.3.10)
Atos Unify First Response OpenScape Policy Store (fix planned for 01/2022)
Atos Unify OpenScape Voice (simplex deployments, fix for embedded OS UC planned for V10 R2)
Atos Unify OpenScape Contact Center V9 and higher
Atos Unify OpenScape Contact Media Service V9 and higher

Confirmed not affected products

Circuit
Atos Unify OpenScape SBC
Atos Unify OpenScape Branch
Atos Unify OpenScape BCF
Atos Unify OpenScape Desk Phones / OpenStage Phones
Atos Unify First Response Emergency Services Applicaction
Atos Unify OpenScape Cordless IP
Atos Unify OpenScape Voice Trace Manager
Atos Unify OpenScape 4000 and Manager
Atos Unify OpenScape Alarm Response
Atos Unify OpenScape Xpert Clients
Atos Unify OpenScape Xpert MLC
Atos Unify OpenScape Xpert System Manager
Atos Unify OpenScape Accounting Management
Atos Unify OpenScape Deployment Service
Atos Unify OpenScape Common Management Portal
Atos Unify OpenScape Composer
Atos Unify OpenScape Backup & Recovery
Atos Unify OpenScape Business
Atos Unify OpenScape UC Clients
Atos Unify OpenScape Xpressions
Atos Unify OpenScape Media Server
Atos Unify First Response MSBF
Atos Unify First Response Gemma V2 and V3
Atos Unify Office
Atos Unify OpenScape ESRP
Atos Unify OpenScape Concierge
Atos Unify OpenScape Voice (except simplex deployments)
Atos Unify OpenScape License Management CLA/CLM
Circuit Meeting Room
Atos Unify OpenScape Fault Management
Atos Unify OpenScape DECT Phones S6/SL6
Atos Unify OpenScape WLAN Phone Wireless Service Gateway
Atos Unify OpenScape WLAN Phone WL4
Atos Unify OpenScape Sesap
Atos Unify OpenScape Contact Center Extensions V3R1

Products under investigation

Atos Unify OpenScape Enterprise Express

Recommended Actions

General Recommendations:

- Focus on internet connected systems first
- Check whether system is running log4j version 2.0 to 2.14.1
- For non-Atos Unify products contact your system or software vendor to validate if log4j is in use and if any additional actions are required

For affected Atos Unify products

- Check whether a system may be compromised. To detect compromise, perform log check as following link
- If you have network monitoring tools in place implements suitable rules in order to detect potential attacks
- If you identify a system being compromised report it to the respective Security Officer or IT manager and consider disconnecting it from the network

Workarounds:

- There is a workaround available for OpenScape V10 and OpenScape Voice V10 (simplex deployment) described in the Knowledge Base Article KB000102509 within the Support Portal (AWSP, registered users only)

References

Important links:
https://www.lunasec.io/docs/blog/log4j-zero-day/
https://github.com/lunasec-io/lunasec/blob/master/docs/blog/2021-12-09-log4j-zero-day.md
https://twitter.com/P0rZ9/status/1468949890571337731
https://logging.apache.org/log4j/2.x/download.html
https://github.com/Neo23x0/log4shell-detector
https://www.tenable.com/cve/CVE-2021-44228
https://supportcenter.us.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176884
https://blog.netlab.360.com/threat-alert-log4j-vulnerability-has-been-adopted-by-two-linux-botnets/

'

General 3rd party Advisories:
https://www.ringcentral.com/trust-center/security-bulletin.html
https://support.polycom.com/content/dam/polycom-support/global/documentation/plygn21-08-poly-systems-apache.pdf
https://github.com/apache/logging-log4j2/pull/608
https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1
https://twitter.com/JLLeitschuh/status/1469148466341416964
https://www.cnblogs.com/yyhuni/p/15088134.html
https://www.veracode.com/blog/research/exploiting-jndi-injections-java
https://issues.apache.org/jira/browse/LOG4J2-2109

https://therecord.media/log4j-zero-day-gets-security-fix-just-as-scans-for-vulnerable-systems-ramp-up/
https://twitter.com/GossiTheDog/status/1469248250670727169
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/
https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2
https://logging.apache.org/log4j/2.x/download.html
https://www.darkreading.com/dr-tech/what-to-do-while-waiting-for-the-log4ju-updates
https://dev.classmethod.jp/articles/aws-waf-new-rule-log4jrce/
https://docs.aws.amazon.com/waf/latest/developerguide/web-request-body-inspection.html
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
https://gist.githubusercontent.com/gnremy/c546c7911d5f876f263309d7161a7217/raw/3a61de8f5d9e74efdffa05cf0bf793e7ca6409bd/CVE-2021-44228_IPs.csv
https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/?s=09
https://security-tracker.debian.org/tracker/CVE-2021-44228
https://www.suse.com/security/cve/CVE-2021-44228.html
https://www.suse.com/c/suse-statement-on-log4j-log4shell-cve-2021-44228-vulnerability/

National Advisories:
https://www.ncsc.gov.uk/news/apache-log4j-vulnerability
https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability
https://www.jpcert.or.jp/at/2021/at210050.html
https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/

Advisory: OBSO-2112-01, status: general release
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com

to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.