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

KB000102509

★ ★ ★ ★ ★ 1546 views

Security Advisory (OBSO2112-01) - Supplementary Information (Atos internal, Registered Customers and Partners)

This information is subject to change, official information will be released on Atos Unify Product Security Advisories and Security Notes (https://unify.com/en/support/security-advisories)

Status	**Pre-Release**
Summary	Apache Log4j2 <= 2.14.1 (excluding the 2.12.2 security release) has a JNDI feature that allows it to look up the content of log messages using names, without any restrictions on what names should be resolved. It does so via various unsafe protocols (e.g. LDAP) that may allow remote code execution. The number CVE-2021-44228 was assigned to this vulnerability, which is also known as “Log4shell”. The vulnerability (CVE-2021-44228) is rated critical with an initial CVSS3 score of 10. On 2021-12-14 it was found that the fix to address CVE-2021-44228 in version 2.15.0 was incomplete in certain non-default configurations, allowing a denial of service (DoS) attack via certain malicious JNDI lookup patterns. The number CVE-2021-45046 was assigned to this vulnerability. The vulnerability (CVE-2021-45046) is rated low with an initial CVSS3 score of 3.7. Versions 2.12.2 and 2.16.0 are addressing both CVEs, mainly by disabling access to JNDI by default, among other countermeasures. Log4j 1.x is not affected by CVE-2021-44228 and CVE-2021-45046. It is, however, affected by a separate JNDI-related vulnerability, which has been given the CVE-2021-4104 and is considered out of the scope of this advisory.
Related KB Articles	• Supplementary information for Atos Unify OpenScape UC V9 and V10 (https://atosunify.service-now.com/kb_view.do?sysparm_article=KB000102540&sysparm_rank=1&sysparm_tsqueryId=0beb6197db900d1003fa120805961906#)
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 code from attacker-controlled domain. • According to security researchers apps and services across the globe have already been actively scanned for vulnerable versions of Log4j by malicious actors. • The vulnerability can be fixed with a configuration change or and update. • Cisco Talos claims to observe threats such as Mirai (https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai) attempting to leverage this vulnerability to automatically infect new systems.

Affected Products	**Product statements are related to product versions before End of Support (M44) is reached** **Confirmed Affected products** Hipath DS-Win version 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 Atos Unify OpenScape Enterprise Express V9 and V10 (Follow instructions for OpenScape UC and OpenScape Contact Center) **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 AC-Win Hipath Cap

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 (https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b) • If you have network monitoring tools in place implement 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:** **For Atos Unify OpenScape UC V10 / Atos Unify OpenScape Voice V10 (simplex deployment):** The instructions to apply this workaround in the openfire (both the embedded and the external openfire) are the following: • Stop openfire with **/etc/init.d/openfire stop** • Edit the startup script **/etc/init.d/openfire** (be sure to keep the same owner and file permissions as before) changing the point where **OPENFIRE_OPTS** variable is defined by adding the JVM argument: **-Dlog4j2.formatMsgNoLookups=true** So the result after the change should be: OPENFIRE_OPTS="${OPENFIRE_OPTS} -DopenfireHome=${OPENFIRE_HOME} -DopenfireLogDir=${OPENFIRE_LOGDIR} -Dopenfire.lib.dir=${OPENFIRE_LIB} -Dlog4j.configurationFile=${OPENFIRE_HOME}/conf/log4j.xml **-Dlog4j2.formatMsgNoLookups=true**" Start again openfire with **/etc/init.d/openfire start** **For Atos Unify OpenScape Contact Center V9 and higher** Follow the procedures provided in the workaround: OSCC Log4Shell Protection Procedures V1.1 (sys_attachment.do?sys_id=8ed87bf3dbd8c15003fa12080596191b)
References	**Important links:** https://www.lunasec.io/docs/blog/log4j-zero-day/ (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://www.lunasec.io/docs/blog/log4j-zero-day/) https://twitter.com/P0rZ9/status/1468949890571337731 (https://www.lunasec.io/docs/blog/log4j-zero-day/) https://logging.apache.org/log4j/2.x/download.html (https://www.lunasec.io/docs/blog/log4j-zero-day/) https://github.com/Neo23x0/log4shell-detector (https://github.com/Neo23x0/log4shell-detector) https://www.tenable.com/cve/CVE-2021-44228 (https://www.tenable.com/cve/CVE-2021-44228) https://supportcenter.us.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176884 (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/ (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://www.ringcentral.com/trust-center/security-bulletin.html) https://github.com/apache/logging-log4j2/pull/608 (https://github.com/apache/logging-log4j2/pull/608) https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1 (https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1) https://twitter.com/JLLeitschuh/status/1469148466341416964 (https://twitter.com/JLLeitschuh/status/1469148466341416964) https://www.cnblogs.com/yyhuni/p/15088134.html (https://www.cnblogs.com/yyhuni/p/15088134.html) https://www.veracode.com/blog/research/exploiting-jndi-injections-java (https://www.veracode.com/blog/research/exploiting-jndi-injections-java) https://issues.apache.org/jira/browse/LOG4J2-2109 (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://therecord.media/log4j-

	zero-day-gets-security-fix-just-as-scans-for-vulnerable-systems-ramp-up/) https://twitter.com/GossiTheDog/status/1469248250670727169 (https://twitter.com/GossiTheDog/status/1469248250670727169) https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b (https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b) https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/ (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://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2) https://logging.apache.org/log4j/2.x/download.html (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://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://dev.classmethod.jp/articles/aws-waf-new-rule-log4jrce/) https://docs.aws.amazon.com/waf/latest/developerguide/web-request-body-inspection.html (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://docs.aws.amazon.com/waf/latest/developerguide/web-request-body-inspection.html) https://gist.githubusercontent.com/gnremy/c546c7911d5f876f263309d7161a7217/raw/3a61de8f5d9e74efdffa05cf0bf793e7ca6409bd/CVE-2021-44228_IPs.csv (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://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://security-tracker.debian.org/tracker/CVE-2021-44228) https://www.suse.com/security/cve/CVE-2021-44228.html (https://www.suse.com/security/cve/CVE-2021-44228.html) https://www.suse.com/c/suse-statement-on-log4j-log4shell-cve-2021-44228-vulnerability/ (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.ncsc.gov.uk/news/apache-log4j-vulnerability) https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability (https://www.ncsc.gov.uk/news/apache-log4j-vulnerability) https://www.jpcert.or.jp/at/2021/at210050.html (https://www.jpcert.or.jp/at/2021/at210050.html) https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited (https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited) https://nvd.nist.gov/vuln/detail/CVE-2021-44228 https://nvd.nist.gov/vuln/detail/CVE-2021-45046 https://nvd.nist.gov/vuln/detail/CVE-2021-4104 (https://nvd.nist.gov/vuln/detail/CVE-2021-44228) https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/ (https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/) https://kb.cert.org/vuls/id/930724 (https://kb.cert.org/vuls/id/930724)
Additional Information for Atos Unify products	Please be aware that all information about affected or not affected products and solutions will be only provided based on official Unify product/solution names. Subcomponents of the products and solutions will not be listed in the following sections. That means all subcomponents are not affected as well if a Unify product is listed under “Confirmed not affected solutions”. **OpenScape Voice:** OpenScape Voice simplex includes OpenScape UC Openfire which is an affected component and a new OSV V10R2 Image will be produced to deliver the fix. **OpenScape UC:** The OpenScape UC component SyncUC is using the library log4j 2.3, however the exploit for CVE-2021-44228 is not applicable as there is no client interface available with input fields providing this operation.

Professional Services Solutions	**Information about Professional Services Solutions Security Advisory for Professional Services – Solutions Support Note DirX-15** **Note: The following links are accessible from zhe Support Portal (AWSP, registered users only)** • Security Advisory for Professional Services – Solutions (sys_attachment.do?sys_id=f879d2b3db10815003fa12080596196f) • Support Note DirX-15: (sys_attachment.do?sys_id=513c96bfdb10815003fa1208059619fc) **Confirmed affected solutions** • UC Integration Server (hot fix / workaround available) The UC Integration Server includes the following applications: UC Integration Launcher, UC Salesforce Integration. **Confirmed not affected solutions** • OSILA (please consider "Support Note DirX-15 for CVE-2021-44228 " as DirX is part of the solution) • Solution Kit V3 / V3R1 (SK V3/V3.1) • Professional Services – Solutions Framework V4 / V5 (PSSF V4/V5) The solutions SK V3/V3.1 and PSSF V4/V4 include the following applications: Communication Desk, Communication Desk Web, AgentDesktop Web, Agent Realtime View Web, Integration Connector (JAVA / COM), Remote Agent, Reporter Package (Multisite Datacollector and WebScheduler), ACD Control, Dashboard, Name Provider Service, Realtime Board, SalesForce Adapter, SkillManagement and customized Concierge based on Solution Kit V3 and Professional Services – Solutions Framework V4 / V5.
Additional Information	The CERT Cordination Center of the Carnegie Mellon University **provide a list of affected vendors with links to their statements**. Atos Unify is taken part in their coordinated Vulnerability Disclosure produre VU#930724: Apache Log4j allows insecure JNDI lookups (https://www.kb.cert.org/vuls/id/930724) In addition the Nationaal Cyber Security Centrum (NCSC-NL) maintains a list in Github about affected vendor: Log4j overview related software (https://github.com/NCSC-NL/log4shell/blob/main/software/README.md) **Affected 3rd party products** ASC Neo >= 6.3 (Check ASC Partner portal (https://www.asc.de/english/login.html) for details) Poly Systems Security Advisory (https://support.polycom.com/content/dam/polycom-support/global/documentation/plygn-21-08-poly-systems-apache.pdf) **Not Affected 3rd party products** HiMed Mediatrix

Last modified 1 hour ago
Products:
Customers:

★ ★ ★ ★ ★ 1546 views

***** - This article solved my issue without the need to open a ticket
**** - This article helped me close a ticket
*** - It helped me with the issue, but didn't provide a complete solution
** - This article didn't help me much/is missing attachments or links
* - This article is outdated/is missing information/contains an error/has a wrong explanation

Posted by Charles Jackman on 2021-12-14 21:44:54
There is a document for the work arounds for OSCC available from Diego Cassiano that needs to be added to this KB.

Leave a comment...