Hive Pro

THREAT ADVISORY

Apache released a patch to address the critical zero-day vulnerability in log4j

TA202157

Threat Level RED

Updated Date – Dec 29, 2021

A zero-day remote code execution vulnerability, CVE-2021-44228 was discovered in Apache log4j affecting versions 2.0 to 2.14.1. Apache log4j is a java logging package used by millions of applications. Cloud services such as Steam, Apple iCloud and apps such as Apache Struts, Minecraft, VMware, Twitter, Cisco, Google, Amazon, LinkedIn, NetApp, Elasticsearch and many others are found to be vulnerable from this flaw.

The vulnerability tracked as CVE-2021-44228, could allow a remote unauthenticated attacker to execute code on vulnerable system. The attack is possible due to the failure of the system to protect against attacker-controlled LDAP and other JNDI related endpoints by the Java logging library.

In order to exploit this issue attacker should have an accessible endpoint from any of the protocol (HTTP, TCP etc.) which helps in sending the arbitrary code. Also, a log statement which logs the string at the endpoint from the request.

Users can check if their system is affected from this vulnerability, if they can find any of the hashes from the repository in their software inventory. For checking the exploitation attempt use the following command on your Linux systems: “sudo egrep -i -r '\$\{jndi:(ldap[s]?|rmi|dns):/[^\n]+' /var/log/”.

We recommend users to take the following actions :

- For identifying the servers vulnerable to Log4j use the detection tool given by TrendMicro.
- For a list of hashes to help determine if a Java application is running a vulnerable version of Log4j check the NCC Group’s GitHub page.
- For Java 8+: upgrade to 2.17.1 and for Java 7: upgrade to 2.12.4 from the patch link and migration guide available in the references.
- Users can remove the LDAP class from log4j by using the command: “zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class”.
- Set “com.sun.jndi.rmi.object.trustURLCodebase” and “com.sun.jndi.cosnaming.object.trustURLCodebase” to “false” if acceptable on JVM versions to mitigate the vulnerability.
- In PatternLayout in the logging configuration, replace Context Lookups like ${ctx:loginId} or $${ctx:loginId} with Thread Context Map patterns (%X, %mdc, or %MDC).
- Deploy the log4j specific rules in your WAF.
- Block specific outbound Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network traffic.
- Implement log4jail - "A fast firewall reverse proxy with TLS (HTTPS) and swarm support for preventing Log4J attacks“.
- Check for the affected software and their fixes available from the link.

The incomplete patch of CVE-2021-44228 resulted in a new issue being tracked as CVE-2021-45056, which affects the versions 2.0 to 2.12.1 , 2.13.0 to 2.15.0 and has been resolved in 2.16.0. An attacker with control over Threat Context map can craft a malicious code using JNDI lookup pattern which can result in a denial-of-service attack.

Apache Log4j2 is affected by another flaw tracked as CVE-2021-45105 and affects the versions 2.0-alpha1 through 2.16.0, resolved in 2.17.0 and 2.12.3. An attacker with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup which result in a StackOverflowError that will terminate the process.

Hive Pro

THREAT ADVISORY

Another vulnerability CVE-2021-4104 in Log4j 1.2 could allow a remote attacker to execute arbitrary code only if the system is configured to use JMSAppender. An attacker with write access to the Log4j configuration can exploit this flaw by causing the untrusted deserialization of untrusted data.

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (CVE-2021-44832) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.

State-sponsored actors such as Apt35 and Hafnium are actively targeting this vulnerability. Currently, the attackers are using the payloads such as crypto miner Kinsing, Mirai botnet, Tsunami, Khonsari, Dridex malware and post-exploitation frameworks such as Cobalt Strike and Mimikatz. Some ransomware such as Conti and TellYouThePass are also targeting the vulnerability.

The Techniques currently used in the attack are:

T1190 - Exploit Public-Facing Application
T1203 - Exploitation for Client Execution
T1059 - Command and Scripting Interpreter
T1496 - Resource Hijacking
T1498 - Network Denial of Service
T1505 - Server Software Component
T1140 - Deobfuscate/Decode Files or Information
T1553 - Subvert Trust Controls
T1059.001 - PowerShell
T1486 - Data Encrypted for Impact
T1090.004 - Domain Fronting
T1114 - Email Collection
T1550.002 - Pass the Hash
T1210 - Exploitation of Remote Services
T1135 - Network Share Discovery
T1083 - File and Directory Discovery
T1482 - Domain Trust Discovery
T1055 - Process Injection
T1068 - Exploitation for Privilege Escalation
T1498 - Network Denial of Service

Actor Details

Name	Known as	Origin	Target Locations	Target sectors
APT 35	Magic Hound , APT 35 , Cobalt Illusion, Charming Kitten , TEMP.Beanie, Timberworm , TarhAndishan , TA453, Phosphorus	Iran	Afghanistan, Canada, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Morocco, Pakistan, Saudi Arabia, Spain, Syria, Turkey, UAE, UK, USA, Venezuela, Yemen	Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications
Hafnium		China	Worldwide	Banking, Education, Engineering, Financial (Finance), Financial Technology(FinTech), Government, Healthcare, Insurance, Legal, Manufacturing, Technology, Telecommunication, Transportation, Electronics, Defense, NGOs

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name	CWE-ID
CVE-2021-44228	Apache log4j versions 2.0 to 2.14.1	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-400 CWE-502
CVE-2021-45046	Apache log4j versions 2.0 to 2.15.0 excluding version 2.12.2	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j denial of service	CWE-502
CVE-2021-45105	Apache log4j versions 2.0 to 2.16.0	cpe:2.3:a:apache:log4j::*:*:*:*:*:*:*:*	Apache Log4j denial of service	CWE-20 CWE-674
CVE-2021-4104	Apache log4j versions 1.x using JNDI in their configuration	cpe:2.3:a:apache:log4j:1.2:*:*:*:*:*:*:*	Apache Log4j code execution	CWE-502
CVE-2021-44832	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4)	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-74

Indicators of Compromise (IoCs)

Type	Value
IPv4	45.155.205.233, 185.191.32.198, 45.137.155.55, 185.154.53.140, 44.240.146.137, 209.141.41.103, 209.127.17.242, 18.27.197.252, 158.247.216.148
URL	http://45.137.155.55/xmrig.exe, http://45.137.155.55/kinsing, http://45.137.155.55/kinsing2, http://185.154.53.140/mg, http://185.154.53.140/get, http://45.137.155.55/cron.sh, http://62.210.130.250/lh.sh, http://62.210.130.250:80/web/admin/x86_64, http://62.210.130.250:80/web/admin/x86, http://62.210.130.250:80/web/admin/x86_g, http://45.130.229.168:9999/Exploit.class, http://18.228.7.109/.log/log, http://18.228.7.109/.log/pty1, http://18.228.7.109/.log/pty2, http://18.228.7.109/.log/pty3, http://18.228.7.109/.log/pty4, http://18.228.7.109/.log/pty5, http://210.141.105.67:80/wp-content/themes/twentythirteen/m8, http://159.89.182.117/wp-content/themes/twentyseventeen/ldm 4, https://localbitcoins.net/, http://158.247.216.148:80/
MD5	3dfbe75871e218d08328a01c56e1bb42, 1538d8c342e3e2a31cd16e01e3865276, 9cb138881a317a7f49c74c3e462f35f4, dbc9125192bd1994cbb764f577ba5dda, c6e8e6bb0295437fb790b1151a1b107e, b7746b922cf7d7fa821123a226ed36, a191dbc673dc3d5eb1c4736a8278ca57,cf2ce888781958e929be430de173a0f8, 20df80b56b1b6ffc8ca49f8ad3ab7b81, ab80c03c460bd3d6a631fd0cedddef49, d766bd832973a991c5894a3521c9815e, 648effa354b3cbaad87b45f48d59c616, 1e051111c4cf327775dc3bab4df4bf85, 0579a8907f34236b754b07331685d79e, ccef46c7edf9131ccffc47bd69eb743b,51e052eb6032d11b3093fecb901870ea, 6ddd9abdd8775b9e1341861fe13fc10a, c717c47941c150f867ce6a62ed0d2d35, 843413de774035248d597941839e3b82, 844864c45816b10356b730f450bd7037, 7356212c0268bfdf78e089b0b9f3a32d, 0f7c2dd019afcc092fd421ee52431aff, 5b30284b34dcc1912326812c7d2ea723, 4c2ccc2f2a4d4fe71249bad63252f32, eb71a394bcf3e8f83198d51f3f6d7422, bf6935865f63c32c0530a61da9b85d53, 720a3a92e72054dc8d58e229c22bb892, f6e51ea341570c6e9e4c97aee082822b,

Type	Value
SHA256	e5e9b0f8d72f4e7b9022b7a83c673334d7967981191d2d98f9c57dc97b4caae1, 68d793940c28ddff6670be703690dfdf9e77315970c42c4af40ca7261a8570fa, 9da0f5ca7c8eab693d090ae759275b9db4ca5acdbcfe4a63d3871e0b17367463, 006fc6623fbb961084243cfc327c885f3c57f2eba8ee05fbc4e93e5358778c85, 2a68fb75fdfb94a63d666a51111ebf38c5d51844e5002d13cba9839102d67653, 7e9663f87255ae2ff78eb882efe8736431368f341849fec000543f027bdb4512, 397ee39d591abe45648d55feb3aaf98258eda59ccf36b2a6d9bc2198eb2ea2b2, 7937bbe245511e3666b1f90661bc5fff1ae7bcb1cfda1e5aad9976b66d871c7f, 1f09bc7eb818beb01f304e96589e5239d3dc525a7b14ce902386211e4ec20b09, 5621a68c852e0f11a813bbe6cfec2a6419654a31d9da7534fd2a835381f8f90a, 0f5cb7f8c43d3ebf71d7e22a2ac2fb94d0457ffea870daa2c402508caa39aca8, 1de182015b280f40b04faac87424f3ae00db8bc90b3ec5d7c02092d72ca1b21e, e8b2a8d0c3444c53f143d0b4ba87c23dd1b58b03fd0a6b1bcd6e8358e57807f1, 93a9db9e9e617e460c3f27073337693e43639edb4c551c7ded86ec57039a42f8, 063ccf736c2c19ca5db70b8d8a7cf00377899c16023c63fee836bdefadd336c1, 704db1ff3acb38583727ed870f48dc67b70ea9f09882ff56a927a82283d9837d, 4b8e0b70c420d83041629b71404c4d9cb942851a6a0a207b0b353fca4ad289d2, c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a, 6b9e23cb675be370a18a0c4482dc566be28920d4f1cd8ba6b4527f80acf978d3, 3f6120ca0ff7cf6389ce392d4018a5e40b131a083b071187bf54c900e2edad26, 6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b, 7101cb0d0229a3794d7575b619f051dde4eba58eae47756f675d552502e6dbe9, 8fd4416f84d30f0480b2676c0fe3e31ce1e10d5f3d88d10bc6cc3e5d878ba0b2, 2a4e636c4077b493868ea696db3be864126d1066cdc95131f522a4c9f5fb3fec, 63d43e5b292b806e857470e53412310ad7103432ba3390ecd4f74e432530a8a9, c38f0f809a1d8c50aafc2f13185df1441345f83f6eb4ef9c48270b9bd90c6799, 6a8965a0f897539cc06fefe65d1a4c5fa450d002d1a9d5d69d2b48f697ee5c05, 715f1f821d028e165bfa750d73505f1a6136184999411300cc88c18ebfa6e8f7, 19370ef36f43904a57a667839727c09c50d5e94df43b9cfb3183ba766c4eae3d, b55ddbaee7abf1c73570d6543dd108df0580b08f730de299579570c23b3078c0, a3f72a73e146834b43dab8833e0a9cfee6d08843a4c23fdf425295e53517afce, 5c46098887e488d91f42c6d9b93b17b2736c9f4cb5a4a1e476c87c0d310a3f28, 370048d94830f0ebd41b052ef455ae4b5b7ca62cab27d1d8d94fdade67e454d0, b3a6fe5bc3883fd26c682bb6271a700b8a6fe006ad8df6c09cc87530fcd3a778, 776c341504769aa67af7efc5acc66c338dab5684a8579134d3f23165c7abcc00, fe98548300025a46de1e06b94252af601a215b985dad31353596af3c1813efb0, e20806791aeae93ec120e728f892a8850f624ce2052205ddb3f104bbbfae7f80, 2b794cc70cb33c9b3ae7384157ecb78b54aaddc72f4f9cf90b4a4ce4e6cf8984, 6370939d4ff51b934b7a2674ee7307ed06111ab3b896a8847d16107558f58e5b, 1a5550f8c0fd049c03d55ebf6829b65d87e27c785f5c6e968dbd3af2ea5b0b50, c154d739cab62e958944bb4ac5ebad6e965a0442a3f1c1d99d56137e3efa8e40, 0e574fd30e806fe4298b3cbccb8d1089454f42f52892f87554325cb352646049, 8052f5cc4dfa9a8b4f67280a746acbc099319b9391e3b495a27d08fb5f08db81, 8933820cf2769f6e7f1a711e188f551c3d5d3843c52167a34ab8d6eabb0a63ef, 8b1d95123a8da5fc351422aa057b9ec7a954c608570757d644e56c72133ec1ed, 39db1c54c3cc6ae73a09dd0a9e727873c84217e8f3f00e357785fba710f98129, 3025630185ea8a3781422351a8a4d415b3f47ed242a70e53fb0d8755ddd01b63, 5fb63deb96eb24a181a58401882d064fc112036aab52a1126fbf254e07562595, eddcd0d13b461e60a52060fc8b60ddb06c552ff645ee557c40b43052ee35b029, 80faa26a8f697e16f72239936a4ef7863742c78dc2a997abaf3265cda51a5514, 15e7942ebf88a51346d3a5975bb1c2d87996799e6255db9e92aed798d279b36b, 9db49e8da667d03c6f758bafa156d0dccb6433ca3f37b3cd94170f749048b779, b74b2907b3b47fcbdab5054ec3ae8a46c7c330fa60d637e735ce9fe73d9ab687,

Type	Value
SHA256	8933820cf2769f6e7f1a711e188f551c3d5d3843c52167a34ab8d6eabb0a63ef, 6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b, 7e9663f87255ae2ff78eb882efe8736431368f341849fec000543f027bdb4512, eddcd0d13b461e60a52060fc8b60ddb06c552ff645ee557c40b43052ee35b029, 5fb63deb96eb24a181a58401882d064fc112036aab52a1126fbf254e07562595, 15e7942ebf88a51346d3a5975bb1c2d87996799e6255db9e92aed798d279b36b, 776c341504769aa67af7efc5acc66c338dab5684a8579134d3f23165c7abcc00, 8052f5cc4dfa9a8b4f67280a746acbc099319b9391e3b495a27d08fb5f08db81, c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a, 93736b26b43ad75a693b01a8764b5771f234858d3f2fed98ee7c3108994727ae, f2e3f685256e5f31b05fc9f9ca470f527d7fdae28fa3190c8eba179473e20789, 90ee1a8e8f0ea5085b83b8efe174674a93260b599729bf53e1b140e2acc7d26f, 7e81fc39bcc8e92a4f0c1296d38df6a10353bbe479e11e2a99a256f670aae392, c56860f50a23082849b6f06fb769f02d2a90753aa8e9397015d8df991c961644, 0f5cb7f8c43d3ebf71d7e22a2ac2fb94d0457ffea870daa2c402508caa39aca8, 3e6567dab5e7c7c42a02ac47e8c68f61c9c481bbbbe5ddb1c68e86f7370dab45, 95ac2e2cd2caf30829a9588988601067a98f9bb02e0776a8ef2b813f9b4d8992, 9dc313bdf572fc01fe3e38a618a0872599a57053b76955098f5eb9bac90c4791, e8b2a8d0c3444c53f143d0b4ba87c23dd1b58b03fd0a6b1bcd6e8358e57807f1, 1b671c42ed304dc34ba41ac9f7666a251336455894350af40f402c30afd497df, 460b096aaf535b0b8f0224da0f04c7f7997c62bf715839a8012c1e1154a38984, 4d15aa5d68b0e8b081c18d0ee5c06cc1758d17246a8d01b3c8ac48d1ef07610b, df84d3e83b4105f9178e518ca69e1a2ec3116d3223003857d892b8a6f64b05ba, c17e71c7ae15fdb02a4e22df4f50fb44215211755effd6e3fc56e7f3e586b299, 8e1e0ddeb249b9f8331b1562498d2cbd9138ec5e00c55a521d489e65b7ef447d, aef59db50378667cff8b3181421445c59a27932d835d47f016a879ced1f04dd7, afceea7c2fc2d273a60c73d209f4a700b98aa2d8df9740fb0a08c3ae47890539, b61f624589d5ad3584e09f3174f8e3e1ac38958f260eee526b0abaf7389d7932, 1e9962a003e423c0bd217ea674754e4d683df8749575302156f9f3e28f3fe6da, 8abaa521a014cdbda2afe77042f21947b147197d274bf801de2df55b1e01c904, 5c8710638fad8eeac382b0323461892a3e1a8865da3625403769a4378622077e, 6ce1bebcd641892898e3a5c14931b1c85dea779578b9c6b752c0b002c6ea3791
SHA1	7758f16acf29c00c396fa5e8f03856155c89784e, b33df9a29540f764236e76c1ea36e7d75607db84, 98a630440b59e49d20cb1f1e467211ecbf0a8404, 59476879657802689e627a6718ac7ec2c97e5d0a, bf2df8f2813ef4e2cf61ea193e091b808aa854c7, e851126ef41e3dc474238d3160f4b0e7e3bbb7ec, 8611063eefa5cc2bbec29870fb56779192eed454, f568eb59fd37b2fe37db730292594d875d3a11e8, 6feb75ac62120bae1e92ab16184c1eb0b795e4b3, fe7f814841791cddbba37f96a79cb3bf8f26c913, 0194637f1e83c2efc8bcda8d20c446805698c7bc, ca4080486566e2cf828de2b72bca1ae0c3bdd8b7, abb335c12d5eb8a3e9fc4c5156c599a0682b7c0b, 38c56b5e1489092b80c9908f04379e5a16876f01, 3379e4778637ad8ba7aac2cab9da36f3a26598ad, 1728f5e2b9abc33184c9b652041b2f438d7ff991, 0d5c6785318e04939abc5edbb15956de2f01ded1, 6cdbce4d65a5be9a4d8c55d74b30186991d38de9,
C2	log.exposedbotnets.ru nazi.uy

Hive Pro

THREAT ADVISORY

Patch Link

https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.15.0/
https://logging.apache.org/log4j/2.x/manual/migration.html
https://github.com/apache/logging-log4j2/pull/607/files

References

https://logging.apache.org/log4j/2.x/
https://www.lunasec.io/docs/blog/log4j-zero-day/
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html?m=1
https://cert-agid.gov.it/download/log4shell-iocs.txt
https://otx.alienvault.com/indicator/cve/CVE-2021-44228
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
https://www.huntress.com/blog/rapid-response-critical-rce-vulnerability-is-affecting-java
https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability
https://github.com/mubix/CVE-2021-44228-Log4Shell-Hashes
https://gist.github.com/nathanqthai/01808c569903f41a52e7e7b575caa890
https://github.com/YfryTchsGD/Log4jAttackSurface
https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
https://security.netapp.com/advisory/ntap-20211210-0007/
https://www.vmware.com/security/advisories/VMSA-2021-0028.html
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
https://www.sentinelone.com/blog/cve-2021-44228-staying-secure-apache-log4j-vulnerability/
https://blog.checkpoint.com/2021/12/11/protecting-against-cve-2021-44228-apache-log4j2-versions-2-14-1/
https://blog.netlab.360.com/threat-alert-log4j-vulnerability-has-been-adopted-by-two-linux-botnets/
https://www.oracle.com/security-alerts/alert-cve-2021-44228.html
https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Magic Hound, APT 35, Cobalt Gypsy, Charming Kitten
https://github.com/pravin-pp/log4j2-CVE-2021-45105
https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement
Mitigating Log4Shell and Other Log4j-Related Vulnerabilities | CISA
http://zdnet.com/article/belgian-defense-ministry-confirms-cyberattack-through-log4j-exploitation/
https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/