NETTITUDE
AN LRQA COMPANY

CVE-2021-44228

Log4Shell

Threat Intelligence Report

Date: 14/12/2021
Version: 1.0

Contents

1 Overview and Context

1.1 Latest Information:

The key characteristics of this vulnerability are:

- **Ease of exploitation:** What makes CVE-2021-44228 especially dangerous is how easy it is to exploit. Someone who is an inexperienced hacker can successfully execute this attack simply by sending a single request that forces a log entry to be written. This will then enable the attacker to upload their own code into the application.
- **The prolific use of Apache Web Servers and the Log4j library:** This library is used in millions of websites, applications and platforms, including a wide range of Apache products. It is also used in gaming platforms such as Minecraft.
- **Proof of concept code exists now and proactive scanning has started already:** The issue was discovered on 9 December and active scanning for this vulnerability started almost immediately. Vulnerability scanning tools have been updated to detect this issue and security products and tools themselves are being patched (where fixes are available).

Overnight (13 Dec) more intelligence emerged around how this vulnerability affects systems:

- **Log4j can be hard to find:** Simply running scanning tools is not always effective in detecting where in networks and products Log4j is used. As it's open-source this means it is very easily incorporated into products. It has been downloaded from the Apache website over 84 million times in the last 4 months alone.
- **Critical importance of asset inventories:** This highlights the vital importance of having robust asset inventories of your products and systems so that you can quickly respond to issues like this.
- **Vendors and Developers are struggling to remediate quickly:** There is a key reliance of vendors and product owners to respond quickly with remediation, fixes, and patching. Many large product vendors are struggling to respond within the timescales required meaning that clients systems remain vulnerable long after the exploits are widely known and used.

1.2 What are we likely to see?

- **Ransomware Initial Access Brokers (IABs) gaining access to systems and then selling this on:** A flurry of activity will likely follow in the next 24-48 hours (Monday, 13 December onwards) as those involved in the Ransomware-As-A-Service (RaaS) supply chain, such as Initial Access brokers, will look to establish persistence before then selling the access on to those skilled in the later stages of kill chain activity.

- **Sophisticated Nation-State threat actors are likely to have a slightly delayed response:** Firstly, while they assess their own exposure, secondly until they have conducted their planning estimate and identified use cases for the exploit in meeting their collection goals.
- **Use of this vulnerability in wormable malware:** Of additional concern is that there is a high 'worm' potential from Log4Shell, and automated exploitation is likely.
- **Signature driven detections will be bypassed:** Although numerous indicators of activity are currently seen, threat actors are also experienced at evading signature driven detections, therefore layered defence strategies will assist with identifying possible second-stage exploitation activity.

2 Activity of Interest

The following details have been observed since the distribution of the initial Nettitude Log4Shell Threat Intelligence Report (13 Dec 2021):

1.3 Possible Earlier Exploitation Dates:

Both Cisco and Cloudflare said they first saw signs of Log4Shell exploitation two weeks before the flaw was made public, meaning security teams need to broaden their incident response investigations and check for signs of possible exploitation against their networks to the start of the month, not just last week. More exactly, the first attacks were seen on 1 Dec 2021.

1.4 How Have Things Developed Since the Last Report?

The disclosure of CVE-2021-44228 (Log4Shell), a remote code execution (RCE) vulnerability residing in Apache Log4j 2, has put thousands of products at risk of exploitation. Some of these products include services provided by common cloud service providers (CSPs), leaving CSP customers vulnerable to remote code execution and prompting rapid update deployments from Google, Microsoft, and Amazon, among other providers.

Of the main 3 CSPs, AWS services currently appear to be the most susceptible to this vulnerability, based on a recently published update demonstrating that at least 13 AWS services are susceptible to CVE-2021-44228. While some of these issues have been resolved server-side, some AWS infrastructure is still awaiting patching, and other mitigations or workarounds must be applied by the client in order to secure AWS deployments using log4j 2.

A similar advisory was released by Google, stating that 4 services are known to be vulnerable to CVE-2021-44228; however, Google is addressing these issues server-side, with some services already patched and others being investigated. Additionally, Google noted that Cloud Armor and Cloud IDS services offered by Google have been updated with rules that aim to identify threat actors' attempts to exploit CVE-2021-44228. Reports from Microsoft demonstrate that Azure services are, at the time of writing, unaffected by this vulnerability.

Other popular CSPs or entities that provide products commonly used with cloud services, such as IBM and Docker, have reported that multiple services and products are vulnerable to CVE-2021-44228, and are following

remediation efforts similar to those described above. At this point, many cloud providers are still attempting to identify server-side vulnerabilities in their products and services, and it is likely that future security bulletins will be released with further client-side recommendations and mitigations. At this time, all sources are suggesting that users update log4j 2 to version 2.15 as soon as possible.

Also of interest at the moment is CVE-2021-42278 and CVE-2021-42287:

On 12 December 2021, @ShitSecure shared a PowerShell implementation to exploit CVE-2021-42287 and CVE-2021-42278. CVE-2021-42287 and CVE-2021-42278 are vulnerabilities affecting Microsoft's Active Directory Domain Services that allow for privilege escalation. The exploit was originally published by @exploitph and automated by @cube0x0. The implementation shared by @ShitSecure allows a user to execute @cube0x0's exploit from memory via PowerShell. The PowerShell implementation is available on GitHub Gist, which can be found linked in the Validation URL section of this note. This vulnerability was addressed as part of the November Patch Tuesday remediations.

Theoretically, it would be possible to use Log4Shell for access than either of these vulnerabilities to achieve Domain Admin, potentially giving threat actors the opportunity to achieve the fabled initial compromise to ransomware delivery in 1 hour.

Although this has been called out on Twitter several times, we are yet to see credible evidence of this being daisy-chained.

Yesterday we made the initial assessment that we were expecting a spike in Initial Access Broker (IAB) activity for RaaS groups. As a TTP development, these IABs have been seen by security researcher Ankit Anubhav conducting 'headcounts' before then auctioning off the access they have established to victims' networks. They were observed using PowerShell to query LDAP via ADSISearcher to see how many individuals had logged on to the domain in the last 100 days (Ankit Anubhav on Twitter). This 'headcount' can then be used to establish a listing price for the access, as well as being used by the RaaS operators to establish potential 'pay off' for pursuing access into these victim environments.

Due to the widespread coverage of the Log4Shell vulnerability, IAB's are now in a race against time to secure the access they have before industry remediation limits their access.

1.5 NCSC Advice

The NCSC are regularly updating their advice and is available here:

- https://www.ncsc.gov.uk/news/apache-log4j-vulnerability

They point to a number of additional detection methods available here:

- https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

Their advice remains that any affected UK organisations should report any evidence of compromise relating to this vulnerability to the NCSC via their website reporting a cybersecurity incident.

The NCSC is aware of widespread scanning for this vulnerability, and they note that almost all organisations will have received HTTP requests with the JNDI string. They do **not** require reports of scanning activity. However please notify the NCSC of any cases where you have identified malicious Java being loaded into one of your systems, or where any follow-on activity has occurred.

1.6 CISA Advice

The US Cybersecurity and Infrastructure Security Agency (CISA) have told federal civilian agencies to patch systems affected by the Log4Shell vulnerability by Christmas Eve. The agency has added yesterday the Log4Shell bug (CVE-2021-44228) to its catalogue of actively-exploited vulnerabilities, along with 12 other security flaws. According to this catalogue, federal agencies have ten days at their disposal to test which of their internal apps and servers utilise the Log4j Java library, check if systems are vulnerable to the Log4Shell exploit, and patch affected servers.

In addition, CISA has also launched yesterday a dedicated web page providing guidance to the US public and private sector regarding the Log4Shell vulnerability.

CISA guidance

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

CISA plans to list all software vendors that have products vulnerable to the Log4Shell vulnerability in the following GitHub page; in order to provide a central place where companies can get Log4Shell patching information. Patches for the Log4j library itself have been available since last week, but software vendors must also incorporate these patches into their own software as well.

GitHub vulnerable vendor list

- https://github.com/cisagov/log4j-affected-db

At the time of writing, this page is currently empty, as the CISA staff are still gathering information

1.7 CSA Singapore Advice

CSA Singapore advice echoes the statements made by other organisations and has a list of immediate actions to consider here:

- https://www.csa.gov.sg/singcert/Advisories/ad-2021-010

1.8 List Of Vulnerable Vendors

The following pages have compiled lists of either vulnerable vendors or listed their public responses so far:

- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/

2 Additional Indicators

Additional Indicators are now available via call-back addresses for Log4Shell scanning. Not all these addresses are malicious, as some are being used by security researchers to index vulnerable hosts. However, these can be a useful starting point for investigating any internet-facing hosts that are vulnerable.

Nettitude recommends inspecting outbound LDAP, HTTP, and RMI (a custom Java protocol typically used on port 1099) traffic as a starting point to triage internet-facing hosts that may be exploited.

2.1 Domains

dns.1433.eu.org
li466-34.members.linode.com
dns.cyberwar.nl
dataastatistics.com
dnslog.xvnming.org.cn
log4j.leakix.net
requestbin.net
bingsearchlib.com
whatis.contentkingapp.com
dnslog.cn
c6rc6225opigvu4t3vn0cg5tqaayyg4ko.dumpp.tk
c6rc6225opigvu4t3vn0cg5x9tayyr7bw.dumpp.tk
interactsh.com
c6rc6225opigvu4t3vn0cg5trxeyygcsn.dumpp.tk
bxss.me
c6rc6225opigvu4t3vn0cg5tg7eyygxu4.dumpp.tk
li826-29.members.linode.com
susu-730.spaces.live.com.alt.rwrxpuqc9askw2wuhxrkis8bi2ozco.burpcollaborator.net
gezimhalili.spaces.live.com.alt.rwrxpuqc9askw2wuhxrkis8bi2ozco.burpcollaborator.net
119.w528fbh7usnhk6fvfaozszdrjip8dx.burpcollaborator.net
196.w528fbh7usnhk6fvfaozszdrjip8dx.burpcollaborator.net
2019.705ka2w8238xwb5ok055wsjl8ce42t.burpcollaborator.net
2019.e2hzjnzvrrp87wbs5imqpkchl8ryfn.burpcollaborator.net
breastsurgeons.org.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
cedexis.com.1uwfvlo0gk65rvo5a5nzs284qvwlka.burpcollaborator.net
hindustanuniv.ac.in.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
museumsusa.org.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
ppts.com.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
meliacuba.com.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
getecsl.com.jg33feb5c7b2ui8djt4bb9dntez6nv.burpcollaborator.net
scanworld.net
log4shell-generic-i2yy0x1rpstssduqpwnm.w.nessus.org
canarytokens.com
binaryedge.io
blueteam.icu
log4shell.huntress.com

2.2 IP Addresses

152.89.239.12	81.30.157.43	217.79.189.13
163.172.157.143	185.250.148.157	78.31.71.248
45.130.229.168	194.195.118.221	78.47.140.224
45.83.193.150	82.118.18.201	80.71.158.12
167.172.44.255	193.3.19.159	92.242.40.21
45.155.205.233	134.209.163.248	62.182.158.156
80.71.158.44	79.172.214.11	45.83.64.1
5.255.97.172	67.205.191.102	167.71.13.196
139.59.175.247	195.54.160.149	172.111.48.30
93.189.42.8	167.86.70.252	31.6.19.41
205.185.115.217	193.201.9.212	161.35.0.78

3 Revision History

Version	Issue Date	Issued by	Comments
1.0	13 Dec 2021	Nettitude Threat Intelligence	Initial Release

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com