FINISHED INTELLIGENCE REPORTS

Log4Shell Malware Analysis Report

TLP:WHITE

Jul 29, 2022

On July 28, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) issued a Malware Analysis Report (MAR), MAR-10386789, regarding their response to an organization that was compromised by exploitation of an unpatched and unmitigated Log4Shell vulnerability in a VMware Horizon server.

All members are encouraged to review Malware Analysis Report (AR22-203A): MAR-10386789-1.v1 - Log4Shell for the full report details and established YARA rules.

The Indicators of Compromise associated with this report have been entered into Health-ISAC's automated sharing platform for members ingesting automated threat indicators.

Upon the disclosure of the critical Log4Shell vulnerability, both opportunistic and highly skilled threat actors have exhibited an increased appetite for the exploitation of systems affected by the security flaw. Since December 2021, the cyber threat landscape has been plagued by multiple threat actors targeting and exploiting Log4Shell on unpatched, public-facing VMware Horizon and Unified Access Gateway (UAG) servers.

From May through June 2022, CISA provided remote incident support at an organization where CISA observed suspected Log4Shell PowerShell downloads. During remote support, CISA confirmed the organization was compromised by malicious cyber actors who exploited Log4Shell in a VMware Horizon server that did not have patches or workarounds applied. CISA analyzed five malware samples obtained from the organization's network, including two malicious PowerShell files, two Extensible Markup Language (XML) files, and a 64-bit compiled Python Portable Executable (PE) file.

The two PowerShell files are Trojan downloaders designed to download malicious files from a command and control (C2) server and install them on the compromised system. One of the scripts also checks for and installs Nmap if it is not installed on the compromised system. The two XML files are for scheduling tasks for persistence. The 64-bit compiled Python PE file is designed to perform scans for IP addresses of live hosts, open ports, and services running on those hosts.

Indicators of Compromise:

- 1d459b9909adf98690635c62ea005009ede8eb9a665b8703fe2ad0b0c414816b (this.ps1)
- 4cdd06a36858ac32a09606bfecb54b517ad41a6aac1e37ca56bb1c193f8174cf (RuntimeService.exe)
- 76a2979d965d42f99558ca6ecd97734697249667291a3013d611e310a03f550e (ps.ps1)
- c357879e2c1013dcf999bcdc65372eacf0895af4a4b4bad2b7d28108d3e7c46a (this.xml)
- e3d2e6b5cd422de1be7e6aa830b91115d204ba5e87c77b6431f3313e0930a697 (that.xml)

Additional Files

- 3b4d726bd366e7439367fa78a186dfa9b641d3b2ad354fd915581b6567480f94 (nmap.exe)
- 407d60626707baee29fb9f2597dd32cfd544ff46df7f76e51ff0b79b3ffce3f2 (this.xml)
- 42c844c62ad1b7ae1925973a9b6845b40d4f626a4895cba9ae9e3e3de3f7973a (n.zip)
- 6408217e10fac9f6549ffaaab328bcfeed4a7ebea71f3dcf60f6186e1b21b501 (that.xml)
- 817046c4fe89cd44dbb613cdac2f0c165e2b47d2b5245911ca6fabdda89d1691 (this.ps1)
- b050749c87399f9978cc6eaea7d25405fc0d099a14c169f5c5f63b8b6ec98b0f (RuntimeService.exe)
- e6bc8aa44233312058704b4d5954c45b4160841f470dd7f6d13c08940e61a7bb (ps.ps1)
- fb833ecd1b1050304f364f879b8b1f7b7136e9c4a21aaf0a6c6b3f419e892d6d (elasticsearch.nse)

Reference(s)	CISA, Health-ISAC
Report Source(s)	CISA

Recommendations
CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special

Publication 800-83, "Guide to Malware Incident Prevention & Handling for Desktops and Laptops"

Release Date
Jul 29, 2022

Sources
MAR-10386789-1.v1 – Log4Shell

NIST Special Publication 800-83, Guide to Malware Incident Prevention & Handling for Desktops and Laptops

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

Threat Indicator(s)

SHA256:
3b4d726bd366e7439367fa78a186dfa9b641d3b2ad354fd915581b6567480f94
e6bc8aa44233312058704b4d5954c45b4160841f470dd7f6d13c08940e61a7bb
e3d2e6b5cd422de1be7e6aa830b91115d204ba5e87c77b6431f3313e0930a69
7
817046c4fe89cd44dbb613cdac2f0c165e2b47d2b5245911ca6fabdda89d1691
c357879e2c1013dcf999bcdc65372eacf0895af4a4b4bad2b7d28108d3e7c46a
1d459b9909adf98690635c62ea005009ede8eb9a665b8703fe2ad0b0c414816b
4cdd06a36858ac32a09606bfecb54b517ad41a6aac1e37ca56bb1c193f8174cf
42c844c62ad1b7ae1925973a9b6845b40d4f626a4895cba9ae9e3e3de3f7973a
6408217e10fac9f6549ffaaab328bcfeed4a7ebea71f3dcf60f6186e1b21b501
b050749c87399f9978cc6eaea7d25405fc0d099a14c169f5c5f63b8b6ec98b0f
407d60626707baee29fb9f2597dd32cfd544ff46df7f76e51ff0b79b3ffce3f2
fb833ecd1b1050304f364f879b8b1f7b7136e9c4a21aaf0a6c6b3f419e892d6d
76a2979d965d42f99558ca6ecd97734697249667291a3013d611e310a03f550e

Alert ID ada51d39

View Alert

Tags log4shell

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.