America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems

Last Revised: July 18, 2022 **Alert Code:** AA22-174A

Summary

Actions to take today:

• Install fixed builds, updating all affected VMware Horizon and UAG systems to the latest versions. If updates or workarounds were not promptly applied following VMware's release of updates for Log4Shell <https://www.vmware.com/security/advisories/vmsa-2021-0028.html> in December 2021, **treat all affected VMware systems as compromised.**

• Minimize the internet-facing attack surface by hosting essential services on a segregated

demilitarized (DMZ) zone, ensuring strict network perimeter access controls, and implementing regularly updated web application firewalls (WAFs) in front of public-facing services

The Cybersecurity and Infrastructure Security Agency (CISA) and United States Coast Guard Cyber Command (CGCYBER) are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders that cyber threat actors, including state-sponsored advanced persistent threat (APT) actors, have continued to exploit CVE-2021-44228 (Log4Shell) in VMware Horizon® and Unified Access Gateway (UAG) servers to obtain initial access to organizations that did not apply available patches or workarounds.

Since December 2021, multiple threat actor groups have exploited Log4Shell on unpatched, public-facing VMware Horizon and UAG servers. As part of this exploitation, suspected APT actors implanted loader malware on compromised systems with embedded executables enabling remote command and control (C2). In one confirmed compromise, these APT actors were able to move laterally inside the network, gain access to a disaster recovery network, and collect and exfiltrate sensitive data.

This CSA provides the suspected APT actors' tactics, techniques, and procedures (TTPs), information on the loader malware, and indicators of compromise (IOCs). The information is derived from two related incident response engagements and malware analysis of samples discovered on the victims' networks.

CISA and CGCYBER recommend all organizations with affected systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities using the IOCs provided in this CSA, Malware Analysis Report MAR-10382580-1 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-174b>, and MAR-10382254-1 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-174a>. If potential compromise is detected, administrators should apply the incident response recommendations included in this CSA and report key findings to CISA.

Update July 18, 2022:

This Cybersecurity Advisory (CSA) has been updated with additional Malware Analysis Report MAR-10382580-2, which provides additional indicators of compromise (IOCs).

Update End

See the list below to download copies of IOCs:

- AA22-174A stix </sites/default/files/publications/aa22-174a.stix.xml>
- MAR-10382254-1 stix </sites/default/files/publications/mar-10382254.r1.v1.white_stix.xml>
- MAR-10382580-1 stix </sites/default/files/publications/mar-10382580.r1.v1.white_stix.xml>
- ***Update July 18, 2022:*** MAR-10382580-2 stix <https://www.cisa.gov/uscert/sites/default/files/mar-10382580.r2.v1.white_stix.xml>

Download the pdf version of this report: [pdf, 426 kb </sites/default/files/publications/aa22-174a_joint_csa_malicious_cyber_actors_exploiting_log4shell_in_unpatched_vmware_horizon_systems_final.pdf>]

Technical Details

Note: this advisory uses the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v11/matrices/enterprise/> framework, version 11. See Appendix A for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques.

Log4Shell is a remote code execution vulnerability affecting the Apache® Log4j library and a variety of products using Log4j, such as consumer and enterprise services, websites, applications, and other products, including certain versions of VMware Horizon and UAG. The vulnerability enables malicious cyber actors to submit a specially crafted request to a vulnerable system, causing the system to execute arbitrary code. The request allows the malicious actors to take full control of the affected system. (For more information on Log4Shell, see CISA's Apache Log4j Vulnerability Guidance <https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance> webpage and VMware advisory VMSA-2021-0028.13 <https://www.vmware.com/security/advisories/vmsa-2021-0028.html>.)

VMware made fixes available in December 2021 and confirmed exploitation in the wild on December 10, 2021.[1 <https://www.vmware.com/security/advisories/vmsa-2021-0028.html>] Since December 2021, multiple cyber threat actor groups have exploited [T1190 <https://attack.mitre.org/versions/v11/techniques/t1190/>] Log4Shell on unpatched, public-facing VMware Horizon and UAG servers to obtain initial access [TA0001 <https://attack.mitre.org/versions/v11/tactics/ta0001/>] to networks.

After obtaining access, some actors implanted loader malware on compromised systems with embedded executables enabling remote C2. These actors connected to known malicious IP address `104.223.34[.]198`.[2] This IP address uses a self-signed certificate CN: `WIN-P9NRMH5G6M8.` In at least one confirmed compromise, the actors collected and exfiltrated sensitive information from the victim's network.

The sections below provide information CISA and CGCYBER obtained during incident response activities at two related confirmed compromises.

Victim 1

CGCYBER conducted a proactive threat-hunting engagement at an organization (Victim 1) compromised by actors exploiting Log4Shell in VMware Horizon. After obtaining access, threat actors uploaded malware, `hmsvc.exe`, to a compromised system. During malwar installation, connections to IP address `104.223.34[.]198` were observed.

CISA and CGCYBER analyzed a sample of `hmsvc.exe` from the confirmed compromise. hmsvc.exe masquerades as a legitimate Microsoft® Windows® service (SysInternals LogonSessions software) [T1036.004 <https://attack.mitre.org/versions/v11/techniques/t1036/004/>] and appears to be a modified version of SysInternals LogonSessions software embedded with malicious packed code. When discovered, the analyzed sample of hmsvc.exe was running as `NT AUTHORITY\SYSTEM`, the highest privilege level on a Windows system. It is unknown how the actors elevated privileges.

`hmsvc.exe` is a Windows loader containing an embedded executable, `658_dump_64.exe`. The embedded executable is a remote access tool that provides an array of C2 capabilities, including the ability to log keystrokes [T1056.001 <https://attack.mitre.org/versions/v11/techniques/t1056/001/>], upload and execute additional payloads [T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>], and provide graphical user interface (GUI) access over a target Windows system's desktop. The malware can function as a C2 tunneling proxy [T1090 <https://attack.mitre.org/versions/v11/techniques/t1090/>], allowing a remote operator to pivot to other systems and move further into a network.

When first executed, `hmsvc.exe` creates the Scheduled Task [T1053.005 <https://attack.mitre.org/versions/v11/techniques/t1053/005/>], `C:\Windows\System32\Tasks\Local Session Updater`, which executes malware every hour. When executed, two randomly named `*.tmp` files are written to the disk at the location `C:\Users\<USER>\AppData\Local\Temp\` and the embedded executable attempts to connect to hard-coded C2 server `192.95.20[.]8` over port `4443`, a non-standard port [TT571 <https://attack.mitre.org/versions/v11/techniques/t1571/>]. The executable's inbound and outbound communications are encrypted with a 128-bit key [T1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>].

For more information on hmsvc.exe, including IOCs and detection signatures, see MAR-10382254-1 <https://cisa.gov/uscert/ncas/analysis-reports/ar22-174a>.

Victim 2

From late April through May 2022, CISA conducted an onsite incident response engagement at an organization (Victim 2) where CISA observed bi-directional traffic between the organization and suspected APT IP address `104.223.34[.]198`. During incident response, CISA determined Victim 2 was compromised by multiple threat actor groups.

The threat actors using IP `104.223.34[.]198` gained initial access to Victim 2's production environment in late January 2022, or earlier. These actors likely obtained access by exploiting Log4Shell in an unpatched VMware Horizon server. On or around January 30,

likely shortly after the threat actors gained access, CISA observed the actors using PowerShell scripts [T1059.001 <https://attack.mitre.org/versions/v11/techniques/t1059/001/>] to callout to `109.248.150[.]13` via Hypertext Transfer Protocol (HTTP) [T1071.001 <https://attack.mitre.org/versions/v11/techniques/t1071/001/>] to retrieve additional PowerShell scripts. Around the same period, CISA observed the actors attempt to download [T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>] and execute a malicious file from `109.248.150[.]13`. The activity started from IP address `104.155.149[.]103`, which appears to be part of the actors' C2 [TA0011 <https://attack.mitre.org/versions/v11/tactics/ta0011/>] infrastructure.

After gaining initial access to the VMware Horizon server, the threat actors moved laterally [TA0008 <https://attack.mitre.org/versions/v11/tactics/ta0008/>] via Remote Desktop Protocol (RDP) [T1021.001 <https://attack.mitre.org/versions/v11/techniques/t1021/001/>] to multiple other hosts in the production environment, including a security management server, a certificate server, a database containing sensitive law enforcement data, and a mail relay server. The threat actors also moved laterally via RDP to the organization's disaster recovery network. The threat actors gained credentials [TA0006 <https://attack.mitre.org/versions/v11/tactics/ta0006/>] for multiple accounts, including administrator accounts. It is unknown how these credentials were acquired.

After moving laterally to other production environment hosts and servers, the actors implanted loader malware on compromised servers containing executables enabling remote C2. The threat actors used compromised administrator accounts to run the loader malware. The loader malware appears to be modified versions of SysInternals LogonSessions, Du, or PsPing software. The embedded executables belong to the same malware family, are similar in design and functionality to `658_dump_64.exe`, and provide C2 capabilities to a remote operator. These C2 capabilities include the ability to remotely monitor a system's desktop, gain reverse shell access, exfiltrate data, and upload and execute additional payloads. The embedded executables can also function as a proxy.

CISA found the following loader malware:

- `SvcEdge.exe` is a malicious Windows loader containing encrypted executable `f7_dump_64.exe`. When executed, `SvcEdge.exe` decrypts and loads `f7_dump_64.exe` into memory. During runtime, `f7_dump_64.exe` connects to hard-coded C2 server `134.119.177[.]107` over port `443`.
- `odbccads.exe` is a malicious Windows loader containing an encrypted executable. When executed, `odbccads.exe` decrypts and loads the executable into memory. The executable attempts communication with the remote C2 address `134.119.177[.]107`.
- `praiser.exe` is a Windows loader containing an encrypted executable. When executed, `praiser.exe` decrypts and loads the executable into memory. The executable attempts connection to hard-coded C2 address `162.245.190[.]203`.
- `fontdrvhosts.exe` is a Windows loader that contains an encrypted executable. When executed, fontdrvhosts.exe decrypts and loads the executable into memory. The executable attempts connection to hard-coded C2 address `155.94.211[.]207`.
- `winds.exe` is a Windows loader containing an encrypted malicious executable and was found on a server running as a service. During runtime, the encrypted executable is decrypted and loaded into memory. The executable attempts communication with hard-coded C2 address `185.136.163[.]104`. `winds.exe` has complex obfuscation, hindering the analysis of its code structures. The executable's inbound and outbound communications are encrypted with an XOR key [T1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>].

For more information on these malware samples, including IOCs and detection signatures, see MAR-10382580-1 <https://cisa.gov/uscert/ncas/analysis-reports/ar22-174b>.

Additionally, CISA identified a Java® Server Pages (JSP) application (`error_401.js`) functioning as a malicious webshell [T505.003 <https://attack.mitre.org/versions/v11/techniques/t1505/003/>] and a malicious Dynamic Link Library (DLL) file:

- `error_401.jsp` is a webshell designed to parse data and commands from incoming HTTP requests, providing a remote operator C2 capabilities over compromised Linux and Windows systems. `error_401.jsp` allows actors to retrieve files from the target system, upload files to the target system, and execute commands on the target system. `rtelnet` is used to execute commands on the target system. Commands and data sent are encrypted via RC4 [T1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>]. For more information on `error_401.jsp`, including IOCs, see [MAR-10382580 2].
- `newdev.dll` ran as a service in the profile of a known compromised user on a mail relay server. The malware had path: `C:\Users\<user>\AppData\Roaming\newdev.dll`. The DLL may be the same `newdev.dll` attributed to the APT actors in open-source reporting <https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits>; however, CISA was unable to recover the file for analysis.

Threat actors collected [TA0009 <https://attack.mitre.org/versions/v11/tactics/ta0009/>] and likely exfiltrated [TA0010 <https://attack.mitre.org/versions/v11/tactics/ta0010/>] data from Victim 2's production environment. For a three week period, the security management and certificate servers communicated with the foreign IP address `92.222.241[.]76`. During this same period, the security management server sent more than 130 gigabytes (GB) of data to foreign IP address `92.222.241[.]76`, indicating the actors likely exfiltrated data from the production environment. CISA also found `.rar` files containing sensitive law enforcement investigation data [T1560.001 <https://attack.mitre.org/versions/v11/techniques/t1560/001/>] under a known compromised administrator account.

Note: the second threat actor group had access to the organization's test and production environments, and on or around April 13, 2022, leveraged CVE-2022-22954 to implant the Dingo J-spy webshell. According to trusted third-party reporting, multiple large organizations have been targeted by cyber actors leveraging CVE-2022-22954 and CVE-2022-

22960. For more information on exploitation of CVE-2022-22954 and CVE-2022-22960, see CISA CSA Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control <https://www.cisa.gov/uscert/ncas/alerts/aa22-138b>.

Incident Response

If administrators discover system compromise, CISA and CGCYBER recommend:

1. Immediately isolating affected systems.
2. Collecting and reviewing relevant logs, data, and artifacts.
3. Considering soliciting support from a third-party incident response organization that can provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
4. Reporting incidents to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). To report cyber incidents to the Coast Guard pursuant to 33 CFR Section 101.305, contact the U.S. Coast Guard (USCG) National Response Center (NRC) (NRC@uscg.mil or 800-424-8802).

Mitigations

CISA and CGCYBER recommend organizations install updated builds to ensure affected VMware Horizon and UAG systems are updated to the latest version.

- If updates or workarounds were not promptly applied following VMware's release of updates for Log4Shell in December 2021 <https://www.vmware.com/security/advisories/vmsa-2021-0028.html>, **treat those VMware Horizon systems as compromised**. Follow the pro-active incident response procedures outlined above prior to applying updates. If no compromise is detected, apply these updates as soon as possible.
  - See VMware Security Advisory VMSA-2021-0028.13 <https://www.vmware.com/security/advisories/vmsa-2021-0028.html> and VMware Knowledge Base (KB) 87073 <https://kb.vmware.com/s/article/87073> to determine which VMware Horizon components are vulnerable.
  - **Note:** until the update is fully implemented, consider removing vulnerable components from the internet to limit the scope of traffic. While installing the updates, ensure network perimeter access controls are as restrictive as possible.
  - If upgrading is not immediately feasible, see KB87073 <https://kb.vmware.com/s/article/87073> and KB87092 <https://kb.vmware.com/s/article/87092> for vendor-provided temporary workarounds. Implement temporary solutions using an account with administrative privileges. Note that these temporary solutions should not be treated as permanent fixes; vulnerable components should be upgraded to the latest build as soon as possible.
  - Prior to implementing any temporary solution, ensure appropriate backups have been completed.
  - Verify successful implementation of mitigations by executing the vendor supplied script `Horizon_Windows_Log4j_Mitigations.zip` without parameters to ensure that no vulnerabilities remain. See KB87073 <https://kb.vmware.com/s/article/87073> for details.

Additionally, CISA and CGCYBER recommend organizations:

- Keep all software up to date and prioritize patching known exploited vulnerabilities (KEVs) <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

- Minimize the internet-facing attack surface by hosting essential services on a segregated DMZ, ensuring strict network perimeter access controls, and not hosting internet-facing services non-essential to business operations. Where possible, implement regularly updated WAFs in front of public-facing services. WAFs can protect against web based exploitation using signatures and heuristics that are likely to block or alert on malicious traffic.
- Use best practices for identity and access management (IAM) by implementing multifactor authentication (MFA), enforcing use of strong passwords, and limiting user access through the principle of least privilege.

Contact Information

Recipients of this report are encouraged to contribute any additional information related to this threat.

- To request incident response resources or technical assistance related to these threats, email CISA at report@cisa.gov. To contact Coast Guard Cyber Command in relation to these threats, email maritimecyber@uscg.mil.
- To report cyber incidents to the Coast Guard pursuant to 33 CFR Section 101.305 contact the USCG NRC (NRC@uscg.mil or 800-424-8802).

Resources

- For more information on Log4Shell, see:
  - CISA's Apache Log4j Vulnerability Guidance <https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance> webpage,
  - Joint CSA Mitigating Log4Shell and Other Log4j-Related Vulnerabilities <https://www.cisa.gov/uscert/ncas/alerts/aa21-356a>, or
  - CISA's database of known vulnerable services <https://github.com/cisagov/log4j-affected-db> on the CISA GitHub® page.

- See National Security Agency (NSA) and Australian Signals Directorate (ASD) guidance Block and Defend Web Shell Malware <https://media.defense.gov/2020/jun/09/2002313081/-1/-1/0/csi-detect-and-prevent-web-shell-malware-20200422.pdf> for additional guidance on hardening internet-facing systems.

References

[1] VMware Security Advisory VMSA-2021-0028.13 <https://www.vmware.com/security/advisories/vmsa-2021-0028.html>

[2] Fortinet's blog New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits <https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits>

Appendix A: Indicators of Compromise

See MAR-10382580-1 <https://cisa.gov/uscert/ncas/analysis-reports/ar22-174b> and MAR-10382254-1 <https://cisa.gov/uscert/ncas/analysis-reports/ar22-174a> and Table 1 for IOCs. See the list below to download copies of these IOCs:

- MAR-10382580-1 stix </sites/default/files/publications/mar-10382580.r1.v1.white_stix.xml>
- MAR-10382254-1 stix </sites/default/files/publications/mar-10382254.r1.v1.white_stix.xml>

Table 1: Indicators of Compromise

Type	Indicator	Description
IP Address	104.223.34[.]198	IP address closely associated with the installation of malware on victims.
	92.222.241[.]76	Victim 2 servers communicated with this IP address and sent data to it during a three-week period.
	109.248.150[.]13	Actors attempting to download and execute a malicious file from this address.
	104.155.149[.]103	Appears to be a part of the actors' C2 infrastructure.

Type	Indicator	Description
Network Port	`192.95.20[.]8:80`	Same description as IP `192.95.20[.]8`, but includes the specific destination port of 80, which was identified in logs and during malware analysis.
	`1389`	This was the most common destination port for Log4Shell exploitation outbound connections. Multiple unique destination addresses were used for Log4Shell callback.
	`104.223.34[.]198:443`	IP address closely associated to the installation of malware on victims with the specific destination port of 443.
Scheduled Task	`C:\Windows\System32\Tasks\Local Session Update`	Scheduled task created by `hmsvc.exe` to execute the program hourly.

Type	Indicator	Description
File Path	`C:\Windows\Temp\lnk{4_RANDOM_CHARS}.tmp`	File created by `hmsvc.exe` with a random four-character filename.
	`C:\Windows\Temp\lnk<4_RANDOM_NUMS_CHAR S>.tmp`	File created by `hmsvc.exe` with a random four-character filename.

Appendix B: Threat Actor TTPs

See Table 2 for the threat actors' tactics and techniques identified in this CSA. See the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v11/matrices/enterprise/> framework, version 11, for all referenced threat actor tactics and techniques.

Table 2: Tactics and Techniques

Tactic	Technique
Initial Access [TA0001 <https://attack.mitre.org/versions/v11/tactics/ta0001/>]	Exploit Public-Facing Application [T1190 <https://attack.mitre.org/versions/v11/techniques/t1190/>]

Tactic	Technique
Execution [TA0002 <https://attack.mitre.org/versions/v11/tactics/ta0002/>]	Command and Scripting Interpreter: PowerShell [T1059.001 <https://attack.mitre.org/versions/v11/techniques/t1059/001/>]
	Scheduled Task/Job: Scheduled Task [T1053.005 <https://attack.mitre.org/versions/v11/techniques/t1053/005/>]
Persistence [TA0003 <https://attack.mitre.org/versions/v11/tactics/ta0003/>]	Server Software Component: Web Shell [T1505.003 <https://attack.mitre.org/versions/v11/techniques/t1505/003/>]
Defense Evasion [TA0005 <https://attack.mitre.org/versions/v11/tactics/ta0005/>]	Masquerading: Masquerade Task or Service [T1036.004 <https://attack.mitre.org/versions/v11/techniques/t1036/004/>]
Credential Access [TA0006 <https://attack.mitre.org/versions/v11/tactics/ta0006/>]	
Lateral Movement [TA0008 <https://attack.mitre.org/versions/v11/tactics/ta0008/>]	Remote Services: Remote Desktop Protocol [T1021.001 <https://attack.mitre.org/versions/v11/techniques/t1021/001/>]

Tactic	Technique
Collection [TA0009 <https://attack.mitre.org/versions/v11/tactics/ta0009/>]	Archive Collected Data: Archive via Utility [T1560.001 <https://attack.mitre.org/versions/v11/techniques/t1056/001/>]
	Input Capture: Keylogging [T1056.001 <https://attack.mitre.org/versions/v11/techniques/t1560/001/>]
Command and Control [TA0011 <https://attack.mitre.org/versions/v11/tactics/ta0011/>]	Application Layer Protocol: Web Protocols [T1071.001 <https://attack.mitre.org/versions/v11/techniques/t1071/001/>]
	Encrypted Channel: Symmetric Cryptography [1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>]
	Ingress Tool Transfer [T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>]
	Non-Standard Port [T1571 <https://attack.mitre.org/versions/v11/techniques/t1571/>]
	Proxy [T1090 <https://attack.mitre.org/versions/v11/techniques/t1090/>]

Disclaimer

Acknowledgements

CISA and CGCYBER would like to thank VMware and Secureworks for their contributions to this CSA.

Revisions

June 23, 2022: Initial version|June 24, 2022: Added link to AA22-174A.stix.xml|July 18, 2022: MAR-10382580-2 stix

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>