SHARING SINCE 2010

H-ISAC®

HEALTH - ISAC

THREAT BULLETINS

Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems

SHARING SINCE 2010 H-ISAC®

HEALTH - ISAC

○○○ TLP:WHITE

Jun 23, 2022

Health-ISAC is distributing the following threat bulletin regarding the Joint Cybersecurity Advisory (CSA) (AA22-174A) released by the Cybersecurity and Infrastructure Security Agency and the United States Coast Guard Cyber Command (CGCYBER) on June 23, 2022. The advisory was released to bring attention to the ongoing exploitation of the Log4Shell vulnerability, identified as CVE-2021-44228, in VMware Horizon and Unified Access Gateway (UAG) servers to gain initial access to organizations that did not apply available patches or workarounds.

According to cybersecurity researchers, several threat actor groups have exploited Log4Shell on unpatched, public-facing VMware Horizon and UAG servers since December 2021. Post-exploitation activity including the deployment of loader malware on compromised systems with embedded executables to enable remote command and control (C2) have been observed.

All members are encouraged to review AA22-174A: Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems for additional information including suspected APT actors' tactics, techniques, and procedures (TTPs), loader malware details, and indicators of compromise (IOCs).

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 webpage and VMware advisory VMSA-2021-0028.13.)

VMware made fixes available in December 2021 and confirmed exploitation in the wild on December 10, 2021. Since December 2021, multiple cyber threat actor groups have exploited Log4Shell on unpatched, public-facing VMware Horizon and UAG servers to obtain initial access to networks.

After obtaining access, some actors implanted loader malware on compromised systems with embedded executables enabling remote C2. These actors are connected to known malicious IP address 104.223.34[.]198. 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 malware 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) 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. The malicious hmsvc.exe acts as 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, upload and execute additional payloads and provide a graphical user interface (GUI) access over a target Windows system's desktop. The malware can function as a C2 tunneling proxy, allowing a remote operator to pivot to other systems and move further into a network.

When first executed, hmsvc.exe creates the Scheduled Task, 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. The executable’s inbound and outbound communications are encrypted with a 128-bit key.

For more information on hmsvc.exe, including IOCs and detection signatures, see MAR-10382254-1.

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 the 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 to callout to 109.248.150[.]13 via Hypertext Transfer Protocol (HTTP) T1071.001 to retrieve additional PowerShell scripts. Around the same period, CISA observed the actors attempt to download 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 infrastructure.

After gaining initial access to the VMware Horizon server, the threat actors moved laterally via Remote Desktop Protocol (RDP) 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 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.

For more information on these malware samples, including IOCs and detection signatures, see MAR-10382580-1.

Additionally, CISA identified a Java® Server Pages (JSP) application (error_401.js) functioning as a malicious webshell T505.003 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. 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; however, CISA was unable to recover the file for analysis.

Threat actors collected and likely exfiltrated 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 under a known compromised administrator account.

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.

Reference(s)	CISA, VMware, CISA, CISA, CISA

Recommendations

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, 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 and VMware Knowledge Base (KB) 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 and KB87092 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 for details.

Additionally, CISA and CGCYBER recommend organizations:

- Keep all software up to date and prioritize patching known exploited vulnerabilities (KEVs).
- 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 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.

Sources
Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems

New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits

Alert ID dd13aee2

View Alert

Tags VMware Unified Access Gateway, log4shell, VMware Horizon

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**.