Hive Pro®

Threat Level

Red

CISA: AA23-325A

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Longstanding Zero-Day in Citrix Devices Exploited Since August

Date of Publication	Last Update Date	Admiralty Code	TA Number
October 19, 2023	November 23, 2023	A1	TA2023424

Summary

First Seen: August 2023
Affected Product: Citrix NetScaler ADC and NetScaler Gateway
Malware: LockBit ransomware
Targeted Countries: Americas, EMEA, and APJ
Targeted Industries: Professional Services, Technology Companies, Legal, Banks, Financial Services, Air Freight & Logistics and Government Organizations
Impact: A zero-day exploit, "Citrix Bleed," identified as CVE-2023-4966, has been actively targeting critical vulnerabilities in Citrix NetScaler ADC/Gateway devices since late August 2023. This exploit has the potential to allow attackers to steal authentication sessions and hijack accounts.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability (Citrix Bleed)	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-4967	Citrix NetScaler ADC and NetScaler Gateway Denial of Service Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓

Vulnerability Details

#1

LockBit ransomware group is exploiting the 'Citrix Bleed' vulnerability, tracked as CVE-2023-4966, to target organizations in the Americas, Europe, Africa, and the Asia-Pacific region. This vulnerability affects Citrix NetScaler ADC/Gateway devices and has been actively exploited as a zero-day vulnerability since late August 2023. The successful exploitation of this flaw could potentially grant unauthorized access to existing authenticated sessions, effectively circumventing multifactor authentication (MFA) and other robust authentication measures.

#2

Citrix has fixed its second zero-day bug in its products this year. The previous one, **CVE-2023-3519**, was discovered in the wild in early July and was patched a few weeks later. Notably, these compromised sessions persist even after applying the security update. Depending on the permissions associated with the compromised account, adversaries can employ this method to laterally traverse the network or breach additional accounts.

#3

This security concern pertains to an information disclosure issue and was rectified just last week. It enables malicious actors to access confidential data in appliances configured as gateways for authentication, authorization, and accounting (AAA) virtual servers. The campaign has targeted professional services, technology companies, legal, and government organizations. More than 10,400 Citrix servers are vulnerable to CVE-2023-4966, with the majority located in the U.S., followed by Germany, China, the U.K., Australia, Canada, France, Italy, Spain, the Netherlands, and Switzerland.

#4

After successfully achieving session hijacking, the threat actor proceeded to conduct post-exploitation activities, which included thorough host and network reconnaissance within the victim's environment, harvesting valuable credentials, and executing lateral movement via Remote Desktop Protocol (RDP). Additionally, the threat actor engaged in Active Directory reconnaissance, utilizing living-off-the-land binaries like net.exe

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-4966	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	CWE-119
CVE-2023-4967			

Recommendations

Prioritize Patching: Upgrade vulnerable NetScaler ADC and Gateway appliances to the latest firmware versions to mitigate the vulnerability. Isolate NetScaler ADC and Gateway appliances for testing and preparation of patch deployment. If immediate patching is not feasible, restrict ingress IP addresses to limit exposure and attack surface.

Credential Rotation: Rotate credentials for users accessing vulnerable NetScaler ADC/Gateway devices as a precaution. If any suspicious activity is spotted or if single-factor remote access is allowed, broaden the credential rotation scope.

Web Shells and Backdoors: In the event of identifying web shells or backdoors on NetScaler appliances, it is advisable to isolate the affected appliances and rebuild them using a clean source image that includes the latest firmware.

Upgrade EOL Versions: Be aware that NetScaler ADC and NetScaler Gateway version 12.1 have reached End-of-Life (EOL). Upgrade to one of the supported versions that address the vulnerabilities.

Vulnerability Management: This entails routinely assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches. Evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1040 Network Sniffing

T1078 Valid Accounts	**T1059** Command and Scripting Interpreter	**T1505** Server Software Component	**T1055** Process Injection
T1135 Network Share Discovery	**T1005** Data from Local System	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities
T1210 Exploitation of Remote Services	**T1563** Remote Service Session Hijacking	**T1548.002** Bypass User Account Control	**T1098** Account Manipulation
T1133 External Remote Services	**T1190** Exploit Public-Facing Application	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1059.006 Python	**T1569.002** Service Execution	**T1027.002** Software Packing	**T1070.004** File Deletion
T1070.006 Timestomp	**T1112** Modify Registry	**T1140** Deobfuscate/Decode Files or Information	**T1620** Reflective Code Loading
T1202 Indirect Command Execution	**T1555.003** Credentials from Web Browsers	**T1003.001** LSASS Memory	**T1115** Clipboard Data
T1560.001 Archive via Utility	**T1007** System Service Discovery	**T1082** System Information Discovery	**T1543** Create or Modify System Process
T1543.003 Windows Service	**T1071.001** Web Protocols	**T1095** Non-Application Layer Protocol	**T1071.004** DNS
T1102 Web Service	**T1489** Service Stop	**T1021.001** Remote Desktop Protocol	**T1482** Domain Trust Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\users\public\adobelib.dll, C:\users\<username>\downloads\process hacker 2\peview.exe, C:\users\<username>\music\process hacker 2\processhacker.exe, C:\perflogs\processhacker.exe, C:\windows\temp\screenconnect\23.8.5.8707\files\processhacker.exe, C:\perflogs\lsass.dmp, C:\users\<username>\downloads\mimikatz.exe, C:\users\<username>\desktop\proc64\proc.exe, C:\users\<username>\documents\veeam-get-creds.ps1, C:\perflogs\64-bit\netscan.exe, C:\perflogs\1.exe, C:\perflogs\run.exe, C:\perflogs\64-bit\m.exe, C:\perflogs\64-bit\m0.exe, C:\perflogs\za_access_my_department.exe, C:\users\<username>\music\za_access_my_department.exe, C:\windows\servicehost.exe, C:\windows\sysconf.bat, C:\windows\temp\screenconnect\23.8.5.8707\files\azure.msi C:\Users\Public\Documents\s.exe, C:\Users\Public\Documents\dsquery.exe, C:\Users\Public\Documents\dsget.exe, C:\Users\Public\Libraries\7z2301-x64.exe, C:\Users\Public\Libraries\mRemoteNG, C:\Users\Public\Libraries\python-3.12.0-amd64.exe
IPv4	192.229.221[.]95, 193.201.9[.]224, 62.233.50[.]25, 51.91.79[.].17, 70.37.82[.]20, 185.17.40[.]178, 185.229.191.41, 81.19.135[.]219, 45.129.137[.]233, 185.229.191[.]41, 172.67.129[.]176, 104.21.1[.]180, 81.19.135[.]220, 81.19.135[.]226, 101.97.36[.]61, 168.100.9[.]137,

TYPE	VALUE
IPv4	185.20.209[.]127, 185.230.212[.]83, 206.188.197[.]22, 54.84.248[.]205, 141.98.9[.]137
File Names	123.ps1, Mag.dll, dns0.org, Temp.sh, Plink.exe, AnyDeskMSI.exe, SRUtility.exe, Netscan.exe, \MEGA\MEGAcmd, Adobelib.dll, rundll32, wmiexec.exe, q0X5wzzEh6P7.hta, psexesvc.exe, secretsdump.py, ad.ps1, tniwinagent.exe, psexec.exe, 7z.exe
URLs	hxxp[://]62.233.50[.]25/en-us/docs[.]html, hxxp[://]62.233.50[.]25/en-us/test[.]html, hxxp[://]81.19.135[.]219/F8PtZ87fE8dJWqe[.]hta, hxxp[://]81.19.135[.]219:443/q0X5wzEh6P7[.]hta
SHA256	9b6b722ba4a691a2fe21747cd5b8a2d18811a173413d4934949047e04e40b30a, 498ba0afa5d3b390f852af66bd6e763945bf9b6bff2087015ed8612a18372155, cc21c77e1ee7e916c9c48194fad083b2d4b2023df703e544ffb2d6a0bfc90a63, ed5d694d561c97b4d70efe934936286fe562addf7d6836f795b336d9791a5c44
Domains	adobe-us-updatefiles[.]digital, assist.zoho[.]eu, eu1-dms.zoho[.]eu, fixme[.]it, unattended.techinline[.]net

Patch Links

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

Recent Breaches

https://allenovery.com
https://icbcfsclearing.com/
https://www.boeing.com/
https://www.dpworld.com/australia
https://nybravestfcu.org
https://brownintegratedlogistics.com
https://sabre.co.uk

References

https://www.tenable.com/blog/cve-2023-4966-citrix-netscaler-adc-and-netscaler-gateway-information-disclosure-exploited-in

https://www.cisa.gov/sites/default/files/2023-11/aa23-325a_lockbit_3.0_ransomware_affiliates_exploit_cve-2023-4966_citrix_bleed_vulnerability.pdf

https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966

https://www.hivepro.com/threat-advisory/citrix-netscaler-adc-and-gateway-vulnerabilities-exploited-in-the-wild/

https://unit42.paloaltonetworks.com/threat-brief-cve-2023-4966-netscaler-citrix-bleed/

https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966

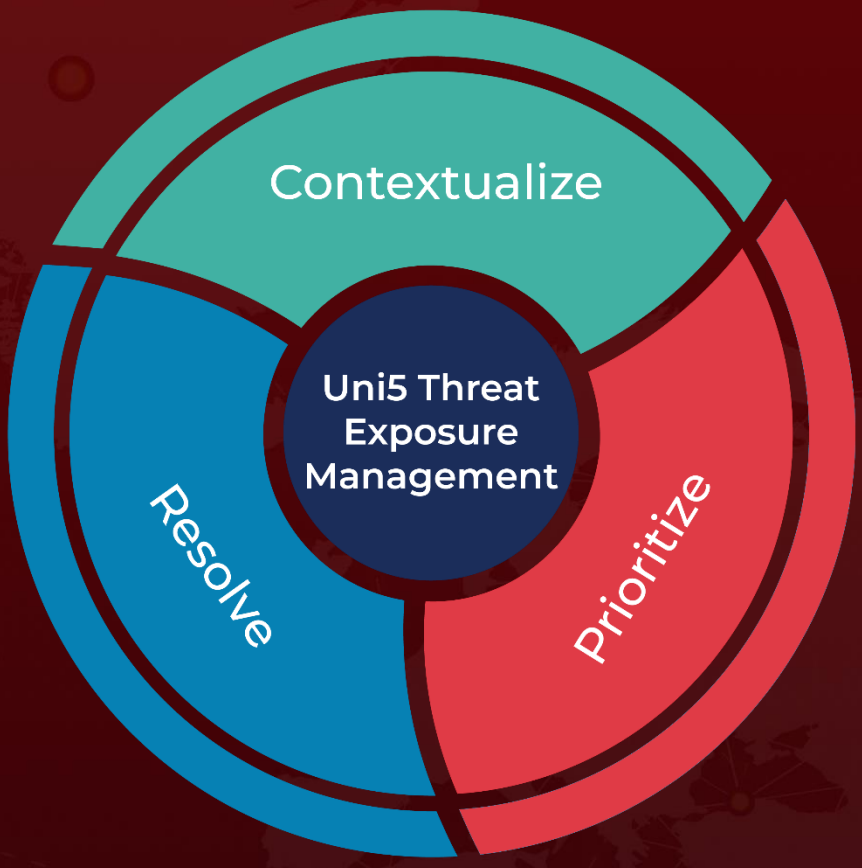
https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-4966

https://doublepulsar.com/lockbit-ransomware-group-assemble-strike-team-to-breach-banks-law-firms-and-governments-4220580bfcee

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 19, 2023 . 5:00 AM

More at www.hivepro.com