Hive Pro

Threat Level

Red

CISA: AA23-201A

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Citrix Netscaler ADC and Gateway Vulnerabilities Exploited in the Wild

Date of Publication	Last updated date	Admiralty Code	TA Number
July 19, 2023	August 3, 2023	A1	TA2023305

Summary

First Seen: July 6, 2023
Affected Product: Citrix ADC and Citrix Gateway
Malware:
Impact: The vulnerabilities in Citrix's Netscaler ADC and Netscaler Gateway, including remote code execution, privilege escalation, and high-risk XSS attacks, can enable unauthorized access, execution of malicious code, and compromise of sensitive data, posing significant risks to affected systems.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-3466	Citrix NetScaler ADC and NetScaler Gateway Cross-Site Scripting Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓
CVE-2023-3467	Citrix NetScaler ADC and NetScaler Gateway Privilege Escalation Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓

Vulnerability Details

#1

Citrix has released a critical security patch to address vulnerabilities in Netscaler ADC and Netscaler Gateway including a severe unauthenticated Remote Code Execution (RCE) flaw (CVE-2023-3519). This vulnerability has already been exploited in the wild. The patch also covers two additional vulnerabilities: a high-severity Reflected Cross-Site Scripting (XSS) flaw (CVE-2023-3466) and a high-severity Privilege Escalation (CVE-2023-3467) vulnerability.

#2

A known threat actor specializing in ransomware attacks is exploiting a vulnerability (CVE-2023-3519) in Citrix NetScaler appliances to drop PHP webshells on victim machines. They uploaded a file with a web shell, scanned the network, and used it to access and steal Active Directory data. They also attempted further actions, like decrypting passwords and implanting a second web shell. The attacker is also using other TTPs, such as domain discovery, plink, BlueVPS hosting, unusual PowerShell scripting, and PuTTY Secure Copy. To be at risk, the appliance must be configured as a Gateway (e.g., VPN, ICA Proxy, CVPN, RDP Proxy) or an AAA virtual server.

#3

Citrix recommends immediate patching, as exploits of CVE-2023-3519 become widespread. The affected products include various versions of NetScaler ADC and NetScaler Gateway, with the fixed versions for each mentioned in the advisory. Upgrading to fixed versions is crucial for maintaining security, especially since the product line is a popular target for attackers, and exploitation is expected to increase rapidly.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID

CVE-2023-3466	NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13;
	NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13;
	NetScaler ADC and NetScaler Gateway version 12.1, now end of life;
	NetScaler ADC 13.1-FIPS before 13.1-37.159;
	NetScaler ADC 12.1-FIPS before 12.1-55.297;
	NetScaler ADC 12.1-NDcPP before 12.1-55.297;
		cpe:2.3:a:citrix:netscaler_application_delivery_controller:11.1-65.22:*:*:*:fips:*:*:*	CWE-20
			CWE-79

CVE-2023-3467			CWE-269
CVE-2023-3519			CWE-94

Recommendations

Apply Patches and Updates: The most crucial step is to apply the patch provided by Citrix. Update the affected systems to the fixed versions mentioned in the security bulletin (e.g., NetScaler ADC and NetScaler Gateway 13.1-49.13 and later releases, NetScaler ADC and NetScaler Gateway 13.0-91.13 and later releases of 13.0, etc.).

Network Segmentation: Isolate the vulnerable systems by implementing network segmentation. This practice helps contain potential attacks and prevents unauthorized lateral movement within the network, minimizing the impact of successful exploitation.

Implement Web Application Firewall (WAF): Deploy a Web Application Firewall in front of the Citrix appliances to protect against reflected cross-site scripting attacks. The WAF can inspect and filter incoming web traffic, adding an extra layer of defense against potential threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0040 Impact	TA0042 Resource Development
TA0004 Privilege Escalation	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	T1531 Account Access Removal
T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation	T1189 Drive-by Compromise	T1090.001 Internal Proxy
T1505.003 Web Shell	T1505 Server Software Component	T1548.001 Setuid and Setgid	T1548 Abuse Elevation Control Mechanism
T1036 Masquerading	T1036.008 Masquerade File Typ	T1552.001 Credentials In Files	T1552 Unsecured Credentials

T1552.004 Private Keys	**T1482** Domain Trust Discovery	**T1069.002** Domain Groups	**T1018** Remote System Discovery
T1016 System Network Configuration Discovery	**T1016.001** Internet Connection Discovery	**T1046** Network Service Discovery	**T1087.002** Domain Account
T1560.001 Archive via Utility	**T1005** Data from Local System	**T1074** Data Staged	**T1105** Ingress Tool Transfer
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell		

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	173-44-141-47[.]nip[.]io
SHA256	ec89ec41f0e0a7e60fa3f6267d0197c7fa8568e11a2c564f6d59855ddd9e1d64, bb28ba8d838c8eefdd5ae1e23d5872968d84e8cb86bf292b2c3bf4c84ad7dbd0, 383df272841f9a677ee03f6f553bc6cf3197427d792dc9f86b7fb1911dc83d71, 20b375ac4487a5955d4b0dd0a600e851d1e455a30c3f8babd0e7e1e97d11a073, 857d6f7e4b96738adb9cc023e2c504362fe8b73bdce422f8f8cb791dd6ac2449, 94f09d01e1397ca80c71b488b8775acfe2776b5ab42e9a54547d9e5f58caf11a, 01717ce6fe0f79c4dc935549c516e4a1941cb4a4e84233e8fdff447177ce556e, 03657d8f9dcb49a690d4b07da4f49ead58000efe458ca3ba7f878233dd25e391, 2d53aaa2638f9a986779b9e36a7b6dfdaddf3cc06698f4aa9f558c1a0591dc9a

TYPE	VALUE
IPv4	45[.]66[.]248[.]189 85[.]239[.]53[.]49
File Path Name	C:\Users\<user>\Downloads\sh[.]ps1, C:\Users\%user%\Documents\gen[.]ps1, C:\Users\%user%\Documents\faf[.]ps1, C:\PerfLogs\Once[.]ps1, C:\PerfLogs\plink[.]exe, C:\PerfLogs\pscp[.]exe, /var/netscaler/logon/LogonPoint/uiareas/%random%[.]php

Patch Details

The vulnerabilities are fixed in the following versions and later releases:
NetScaler ADC and NetScaler Gateway 13.1-49.13 and later releases
NetScaler ADC and NetScaler Gateway 13.0-91.13 and later releases of 13.0
NetScaler ADC 13.1-FIPS 13.1-37.159 and later releases of 13.1-FIPS
NetScaler ADC 12.1-FIPS 12.1-55.297 and later releases of 12.1-FIPS
NetScaler ADC 12.1-NDcPP 12.1-55.297 and later releases of 12.1-NDcPP

Link:
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

https://www.cisa.gov/news-events/alerts/2023/07/18/citrix-releases-security-updates-netscaler-adc-and-gateway

https://www.citrix.com/blogs/2021/04/12/improve-your-security-posture-with-security-advisory-in-citrix-adm-service/

https://www.rapid7.com/blog/post/2023/07/18/etr-critical-zero-day-vulnerability-in-citrix-netscaler-adc-and-netscaler-gateway/

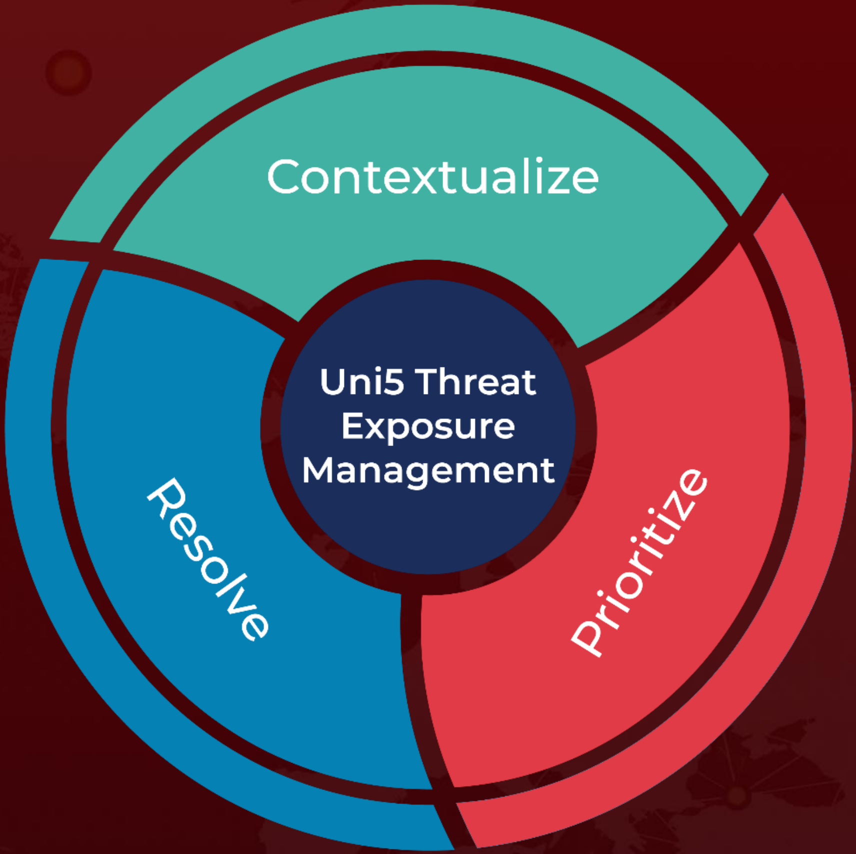
https://twitter.com/SophosXOps/status/1695143572272738790

https://github.com/sophoslabs/IoCs/blob/master/2023-08-25%20Citrix%20CVE-2023-3519%20attacks.csv

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

July 19, 2023 • 6:30 AM

More at www.hivepro.com