Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Citrix Warns of Critical Netscaler Flaws Actively Exploited in Attacks - Urges Immediate Patching

Date of Publication	Admiralty Code	TA Number
January 17, 2024	A1	TA2024020

Summary

First Seen: January 16, 2024
Affected Products: NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway)
Impact: Two zero-day security vulnerabilities, identified as CVE-2023-6548 and CVE-2023-6549, have been discovered in NetScaler ADC and NetScaler Gateway. These vulnerabilities are actively exploited in the wild. CVE-2023-6548 affects the NetScaler management interface, potentially leading to remote code execution, while CVE-2023-6549 exposes unpatched NetScaler instances to denial-of-service attacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-6548	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-6549	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	NetScaler ADC and NetScaler Gateway	✓	✓	✓

Vulnerability Details

#1

Two vulnerabilities, namely CVE-2023-6548 and CVE-2023-6549, have been identified in NetScaler ADC (previously known as Citrix ADC) and NetScaler Gateway (previously known as Citrix Gateway). These vulnerabilities affect the NetScaler management interface and pose risks to unpatched NetScaler instances, leading to potential remote code execution and denial-of-service attacks.

#2 CVE-2023-6548 is a RCE vulnerability which arises from inadequate input validation within the management interface. A remote authenticated user can exploit this vulnerability by sending a specially crafted request to the application, leading to the execution of arbitrary code on the target system. It's important to note that to achieve code execution, attackers must be logged in to low-privilege accounts on the targeted instance and require access to NSIP, CLIP, or SNIP with management interface access.

#3 CVE-2023-6549 is identified as a denial-of-service (DoS) vulnerability. The vulnerability stems from a boundary error. In this scenario, a remote attacker can send specially crafted packets to the system, triggering memory corruption and executing a DoS attack. Successful exploitation of this vulnerability necessitates the device being configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server.

#4 Citrix has reported that these vulnerabilities have been actively exploited in the wild. However, specific details about the in-the-wild exploitation have not been disclosed. As a precautionary measure, administrators who are unable to immediately apply the latest security updates are advised to block network traffic to the affected instances and ensure that these instances are not exposed online.

#5 Another critical vulnerability in NetScaler, identified as CVE-2023-4966 (aka Citrix Bleed), was patched in October. This flaw had been actively exploited as a zero-day by multiple threat groups since August. Organizations are urged to ensure that their systems are updated with the latest security patches to protect against such exploitations.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-6548	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15, NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21, NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	CWE-94
CVE-2023-6549		cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	CWE-119

Recommendations

Apply Patch: Install the security patch provided by Citrix to address the CVE-2023-6548 and CVE-2023-6549 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Block Network Traffic: To enhance security, administrators who are unable to promptly deploy the latest security updates are advised to block network traffic to affected instances and ensure that these instances are not exposed online.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0040 Impact	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1498 Network Denial of Service			

Patch Details

Citrix has released patches for these vulnerabilities for the following versions.
NetScaler ADC and NetScaler Gateway 13.0-92.21 and later releases of 13.0
NetScaler ADC and NetScaler Gateway 13.1-51.15 and later releases of 13.1
NetScaler ADC and NetScaler Gateway 14.1-12.35 and later releases
NetScaler ADC 12.1-55.302 and later releases of 12.1-NDcPP
NetScaler ADC 12.1-55.302 and later releases of 12.1-FIPS
NetScaler ADC 13.1-37.176 and later releases of 13.1-FIPS

Link:
https://www.citrix.com/downloads/

References

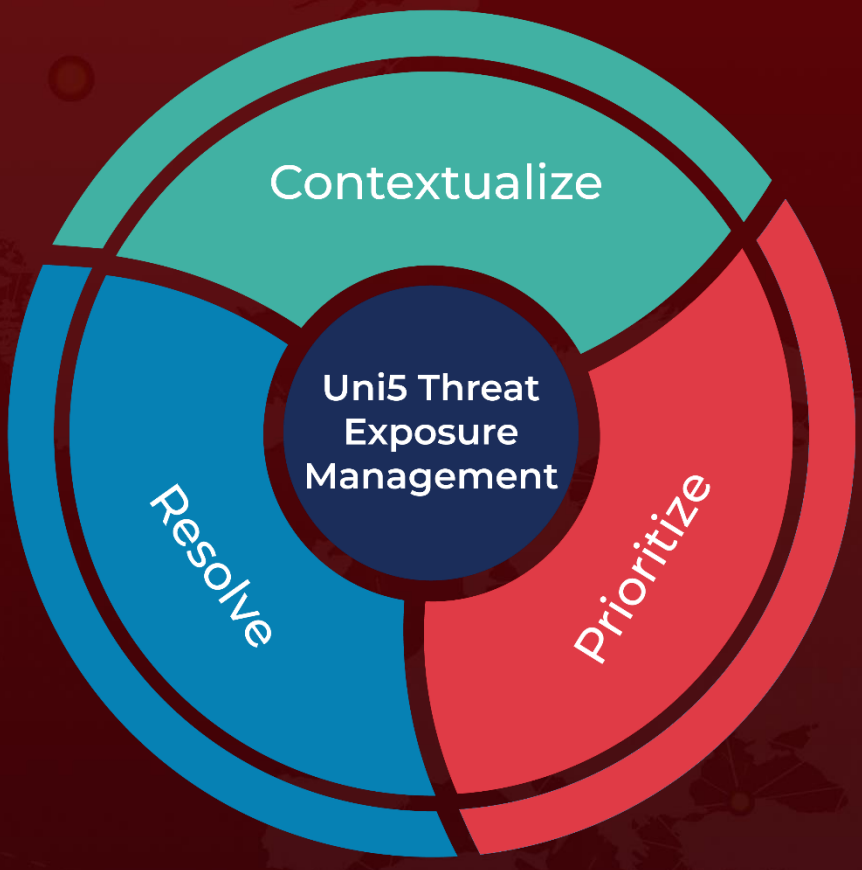
https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549

https://www.hivepro.com/threat-advisory/a-longstanding-zero-day-in-citrix-devices-exploited-since-august/

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

January 17, 2024 • 4:15 AM

More at www.hivepro.com