Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-7775: Actively Exploited Critical Flaw in Citrix NetScaler

Date of Publication

August 28, 2025

Admiralty Code

A1

TA Number

TA2025262

Summary

First Seen: August 2025
Affected Product: Citrix NetScaler ADC and NetScaler Gateway
Impact: Citrix has disclosed three critical vulnerabilities in NetScaler ADC and Gateway (CVE-2025-7775, CVE-2025-7776, CVE-2025-8424), with CVE-2025-7775 already under active exploitation. The flaws allow remote code execution, denial of service, or unauthorized access, and impact multiple versions of NetScaler. There are no workarounds, immediate patching is required to prevent compromise, and service disruption.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-7775	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2025-7776	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓
CVE-2025-8424	Citrix NetScaler ADC and NetScaler Gateway Improper Access Control Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓

Vulnerability Details

#1

Citrix recently disclosed three critical vulnerabilities impacting NetScaler ADC and NetScaler Gateway, CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424. Among these, CVE-2025-7775 is the most severe, as it is a memory overflow vulnerability that allows unauthenticated remote code execution (RCE) or denial of service (DoS). This issue is already being exploited in the wild, making it a critical zero-day threat.

#2

The other two vulnerabilities also pose serious risks. CVE-2025-7776 is another memory overflow bug that can result in service disruption, while CVE-2025-8424 is an access-control weakness tied to the management interface. Although exploitation of these two flaws has not yet been observed, their potential impact on availability and security makes them highly significant. Unlike CVE-2025-7775, however, there is no confirmation of active attacks leveraging them at this time.

#3

Citrix has provided fixes in specific software versions, including 14.1-47.48, 13.1-59.22, 13.1-37.241-FIPS, and 12.1-55.330-FIPS. Users running earlier versions are advised to upgrade immediately, as there are currently no workarounds or mitigations available. Organizations with internet-facing appliances are at especially high risk, since attackers are already exploiting CVE-2025-7775 in real-world campaigns.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-7775	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP	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-2025-7776			CWE-119
CVE-2025-8424			CWE-284

Recommendations

Patch Immediately: Upgrade all affected NetScaler ADC and Gateway appliances to the latest fixed releases. No workarounds exist, so patching is the only effective defense against these vulnerabilities.

Prioritize CVE-2025-7775: This flaw is actively exploited and enables unauthenticated remote code execution. Treat it as critical and patch urgently, or restrict external access until updates are applied.

Audit and Monitor Systems: Continuously review logs and monitor for unusual activity or failed authentication attempts. Deploy intrusion detection and threat hunting to spot potential compromise.

Limit Exposure: Keep management interfaces off the public internet and restrict access to internal networks or VPN. Apply least-privilege principles for all administrative accounts.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0040 Impact	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1588** Obtain Capabilities
T1190 Exploit Public-Facing Application	**T1499** Endpoint Denial of Service	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1203 Exploitation for Client Execution	**T1133** External Remote Services	**T1078** Valid Accounts	

Patch Details

NetScaler ADC and NetScaler Gateway 14.1-47.48 and later releases
NetScaler ADC and NetScaler Gateway 13.1-59.22 and later releases of 13.1
NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.241 and later releases of 13.1-FIPS and 13.1-NDcPP
NetScaler ADC 12.1-FIPS and 12.1-NDcPP 12.1-55.330 and later releases of 12.1-FIPS and 12.1-NDcPP

Link:
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424

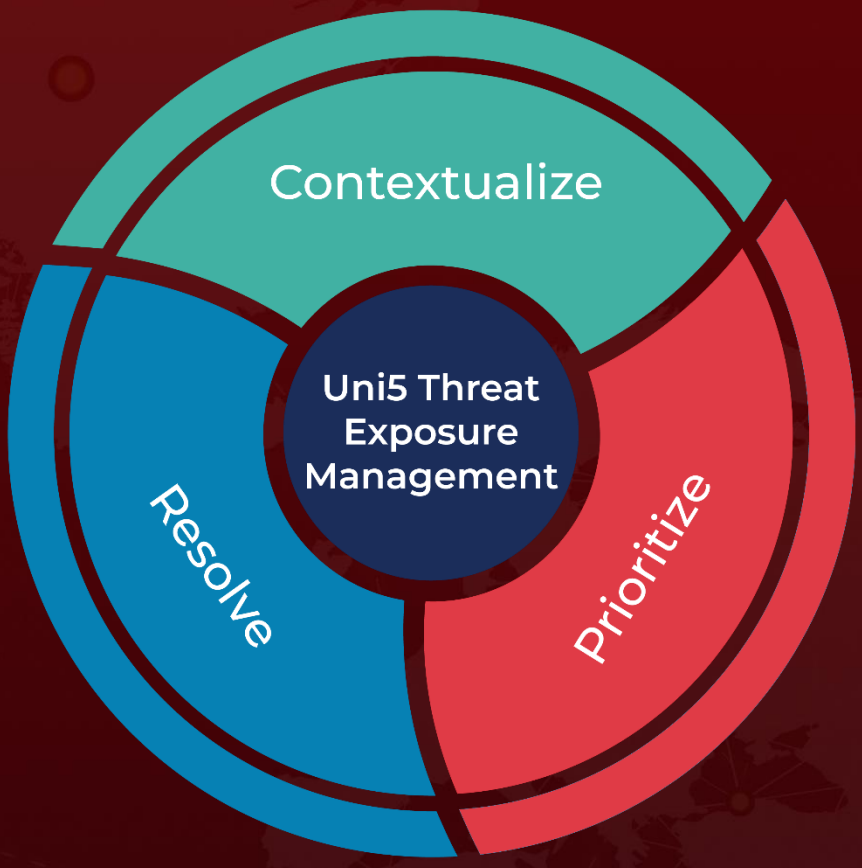
References

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424

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

August 28, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com