Citrix Patches Three Zero Days as One Sees Active Exploitation - Against I

Data: 2025-08-28 09:03:47

Autor: Inteligência Against Invaders

Citrix has released patches for three zero-day vulnerabilities in NetScaler ADC and Gateway, one of which was already being exploited by attackers.

The flaws, tracked as CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424, are two memory overflow vulnerabilities and an improper access control on the NetScaler Management Interface.

They are all considered critical vulnerabilities, with severity score (CVSS) ratings of 9.2, 8.8 and 8.7, respectively.

The following systems are affected by all three vulnerabilities:

- 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

Additionally, Secure Private Access on-prem or Secure Private Access Hybrid deployments using NetScaler instances are also affected by the vulnerabilities.

In an August 26 advisory, Citrix indicated that CVE-2025-7775 had been observed being exploited in the wild on “unmitigated appliances.”

According to independent security researcher Kevin Beaumont, exploit campaigns began before the patches were made avaliable by Citrix.

He stated that CVE-2025-7775, which he dubbed ‘CitrixDeelb,’ is “the main problem, [with] pre-authentication remote code execution (RCE) being used to drop webshells to backdoor organizations.”

Based on initial internet scanning for hosts vulnerable to CVE-2025-7775, Beaumont said he found that 84% affected appliances were vulnerable as of August 26.

Customers Urged to Patch Vulnerable Appliances

Citrix urged users to upgrade to one of the following patched versions:

- 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

No other workaround is available to mitigate the exploitation of one of these vulnerabilities.

The software developer also noted that NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are now considered end-of-life (EOL) versions and are no longer supported.

“Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities,” the Citrix advisory added.

Patching Is Not Enough, Experts Said

Simply applying patches without futher investigation of potential compromise is not sufficient, warned Benjamin Harris, CEO of watchtower.

“Patching is critical, but patching alone won’t cut it. Unless organizations urgently review for signs of prior compromise and deployed backdoors, attackers will still be inside. Those that only patch will remain exposed,” he said.

Caitlin Condon, VP of security research at VulnCheck, argued that exploit campaigns are likely coming from sophisticated threat actors and hinted *at involvement by* nation-state groups.

“Memory corruption vulnerabilities like CVE-2025-7775 and CVE-2025-7776 can be tricky to exploit and on the whole tend to be used by state-sponsored or other skilled adversaries in targeted attacks rather than leveraged by commodity attackers broadly,” she said.

VulnCheck’s research has identified that another recent Citrix NetScaler vulnerability, CVE-2025-6543, which affects a narrower set of configurations, shares a nearly identical description with CVE-2025-7775. However, CVE-2025-6543 has not been exploited at scale despite its inclusion on VulnCheck’s Known Exploited Vulnerabilities (KEV) list since June 25, according to the firm.

While Citrix’s advisory explicitly confirms active exploitation only for CVE-2025-7775, VulnCheck’s Condon warned that “management interfaces for firewalls and security gateways have been targeted en masse in recent campaigns.”

She emphasized the risk of future exploit chains combining an initial access flaw like CVE-2025-7775 with a secondary vulnerability such as CVE-2025-8424, with the ultimate goal of compromising management interfaces.

Condon urged organizations to prioritize patching CVE-2025-8424, cautioning that “vulnerability response shouldn’t focus solely on higher-severity memory corruption CVEs – some of which are harder to exploit – at the expense of more operationally critical flaws.”