VULNERABILITY BULLETINS

Citrix Discloses a Trio of Vulnerabilities Affecting NetScaler ADC and NetScaler Gateway

TLP:WHITE

Aug 26, 2025

On August 26, 2025, Citrix released a security bulletin (CTX694938) to address three critical vulnerabilities affecting its NetScaler ADC and NetScaler Gateway products: CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424.

The most severe of these, CVE-2025-7775, is an actively exploited memory overflow flaw that can lead to remote code execution (RCE) and/or denial of service (DoS). The other two vulnerabilities allow for DoS and improper access control, respectively. Citrix strongly urges all users with affected, user-managed appliances to update to the recommended builds immediately to mitigate these critical risks.

Health-ISAC provides this information to increase situational awareness, encourage users to assess their level of risk to these vulnerabilities, and apply patches to affected instances.

These flaws impact several supported versions of NetScaler ADC and NetScaler Gateway, including 14.1, 13.1, and 12.1. The vulnerabilities are only present on appliances configured as a Gateway, an AAA virtual server, or in specific load balancing configurations involving IPv6 or PCoIP profiles. This bulletin applies

only to customer-managed devices, as Citrix-managed cloud services are automatically updated by the Cloud Software Group.

CVE-2025-7775 is a critical memory overflow vulnerability with a CVSSv4 score of 9.2. It can lead to remote code execution (RCE) and/or denial of service. The vulnerability is exploitable if the NetScaler device is configured as a Gateway or AAA virtual server, or in specific load balancing scenarios with IPv6 services. Citrix has confirmed that this flaw is being actively exploited on unmitigated appliances, highlighting the immediate and severe risk it poses.

CVE-2025-7776 is another memory overflow vulnerability, rated with a CVSSv4 score of 8.8. This flaw can cause unpredictable or erroneous behavior and denial of service. It affects appliances configured as a Gateway (VPN, ICA Proxy, CVPN, RDP Proxy) with a PCoIP Profile bound to it. While not as severe as CVE-2025-7775, the potential for service disruption makes this a high-priority concern for affected organizations.

The third vulnerability, CVE-2025-8424, is an improper access control flaw on the NetScaler Management Interface, with a CVSSv4 score of 8.7. An attacker with access to the NSIP, Cluster Management IP, or a local GSLB Site IP with Management Access could exploit this flaw. This could lead to a compromise of the management interface, potentially allowing the attacker to gain full administrative control over the device.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability. There are no available workarounds or mitigating factors other than applying the official software updates:

- **Upgrade to Fixed Versions:**
  - NetScaler ADC and NetScaler Gateway 14.1 must be updated to 14.1-47.48 or later.
  - NetScaler ADC and NetScaler Gateway 13.1 must be updated to 13.1-59.22 or later.
  - NetScaler ADC 13.1-FIPS and NDCPP must be updated to 13.1-37.241-FIPS and NDCPP or later.
  - NetScaler ADC 12.1-FIPS and NDCPP must be updated to 12.1-55.330-FIPS and NDCPP or later.
- **End-of-Life Products:** NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are EOL and will not receive patches. Customers using these versions are advised to upgrade to a supported version immediately.
- **Inspect and Terminate Sessions:** Given the active exploitation of CVE-2025-7775, users should inspect NetScaler configurations for the preconditions of the vulnerability and take appropriate actions to ensure unauthorized access is revoked.
- **Review the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

Reference(s)	citrix, helpnetsecurity

Alert ID 671361ad

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-8424, CVE-2025-7776, CVE-2025-7775, Citrix, NetScaler Gateway, NetScaler ADC

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**