PoC Exploit Available for Citrix NetScaler ADC and Gateway CVE-2026-8452

Aug 17, 2026

WHITE

View Alert

On August 14, 2026, researchers at watchTowr published a technical write-up and working proof-of-concept (PoC) exploit for CVE-2026-8452 (CVSS 8.8), a pre-authentication vulnerability in Citrix NetScaler ADC and Gateway.

Additional Info

Analysis

CVE-2026-8452 is a memory overflow vulnerability affecting appliances configured as a Gateway or AAA virtual server, which can lead to unpredictable behavior or a Denial of Service (DoS) attack.

With their PoC exploit, watchTowr demonstrated that the flaw, triggered by missing bounds checks during SAML signature canonicalization when copying data, can be weaponized as a write-what-where memory corruption primitive to achieve unauthenticated root code execution.

The issue affects customer-managed NetScaler appliances configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or as an AAA virtual server, running 14.1 builds prior to 14.1-72.61, 13.1 builds prior to 13.1-63.18, and corresponding FIPS/NDcPP releases.

Although Citrix patched its managed cloud services beforehand and no active exploitation in the wild has been confirmed yet, the public availability of exploit code increases the chances of an attack for edge-facing enterprise appliances.

Recommendations

- Ensure the latest Citrix updates have been applied to mitigate the vulnerability.
- Use perimeter firewalls and network access control lists (ACLs) to restrict access to SAML, VPN, and AAA endpoints to trusted IP ranges where feasible until patches are applied.
- Inspect NetScaler system event logs (newnslog) and check /var/core/ for core dumps or unexpected restarts of the NetScaler Packet Engine (nsppe) process that could signal prior exploitation attempts.
- Review SAML authentication configurations and monitor network traffic for unusually large or malformed inbound SAML requests targeting the appliance.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

<hr size=1 width="100%" align=center>

Alert Id	d59468c2
Category	Threat Bulletins
Tags	CVE-2026-8452, Citrix ADC and Gateway

Sources

https://labs.watchtowr.com/youre-back-in-the-room-citrix-netscaler-pre-auth-rce-cve-2026-8452/
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604

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

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--