

Citrix Patches Critical NetScaler ADC and NetScaler Gateway Flaw (CVE-2026-107406)

Oct 09, 2026

○ WHITE

[View Alert](#)

On October 8, 2026, Citrix [disclosed](#) a critical memory overflow vulnerability (CVE-2026-107406) affecting NetScaler ADC and NetScaler Gateway, assigning it a CVSS score of 9.5 out of 10.0.

Additional Info

Analysis

Under specific configuration conditions, an attacker could exploit this flaw to achieve remote code execution (RCE) or trigger a denial-of-service (DoS) state. The flaw was discovered and reported by security researchers.

Vulnerability exposure strictly requires appliances to be actively configured as a SAML Identity Provider (IdP) or Service Provider (SP). While threat intelligence group Shadowserver monitors over 21,000 internet-facing NetScaler IP addresses globally, Citrix reports no known active exploitation in the wild, though NetScaler products remain frequent targets for threat actors.

To eliminate the security risk, Citrix released patched firmware versions across all supported release trains, including standard and FIPS-compliant builds. Because unmitigated vulnerabilities on perimeter devices pose severe risk to corporate networks, immediate assessment and firmware upgrades are required for all instances running SAML authentication services.

Citrix is recommending that its customers immediately apply available updates:

- Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1-73.46 and later releases
- Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1-64.29 and later releases of 13.1
- Citrix NetScaler ADC 14.1-FIPS 14.1-73.46 FIPS and later releases of 14.1-FIPS
- Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1.37.283 and later releases of 13.1-FIPS and 13.1-NDcPP

Recommendations

- Immediately inspect configuration files for add authentication samlAction (SAML SP) or add authentication samldpProfile (SAML IdP) commands to identify vulnerable instances.
- Upgrade affected ADC, Gateway, and FIPS deployments to safe versions.
- Ensure all NetScaler appliances integrated within Secure Private Access Hybrid architectures are included in the patching schedule and brought up to fixed versions.
- Review the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients Resources](#).

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

Alert Id	eb5fab99
Category	Vulnerability Bulletins
Tags	CVE-2026-107406, Citrix ADC and Gateway

Sources

<https://support.citrix.com/external/article/CTX697191/citrix-netscaler-adc-and-citrix-netscale.html>
<https://www.bleepingcomputer.com/news/security/citrix-warns-admins-to-patch-new-netscaler-rce-flaw-immediately/>
<https://thehackernews.com/2026/10/citrix-patches-critical-netscaler-flaw.html>

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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

Please provide your feedback



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

.