Citrix NetScaler Authentication and Session Handling Vulnerabilities Impact Gateway and SAML Services

TL;DR

Two vulnerabilities in Citrix NetScaler ADC and Citrix NetScaler Gateway (CVE-2026-3055 and CVE-2026-4368) impact authentication and remote access components.

The issues affect SAML identity provider configurations and gateway or AAA services, which are commonly exposed to the internet. If exploited, an attacker could interfere with authentication flows or user sessions, potentially gaining access to sensitive systems.

Overview

There are two vulnerabilities (CVE-2026-3055, CVSS 9.3 and CVE-2026-4368, CVSS 7.7) in Citrix NetScaler ADC and NetScaler Gateway that impact how authentication data and user sessions are handled. These systems are often deployed at the edge of the network and are responsible for managing login traffic, VPN access, and identity validation.

Affected Products

- NetScaler ADC 14.1 before 14.1-60.58
- NetScaler ADC 13.1 before 13.1-62.23
- NetScaler ADC FIPS and NDcPP before 13.1-37.262
- NetScaler Gateway (same affected versions as above)
- NetScaler ADC and Gateway 14.1-66.54 (specific to CVE-2026-4368)

CVE-2026-3055 is caused by insufficient input validation and can lead to a memory overread when NetScaler is configured as a SAML identity provider. CVE-2026-4368 is a race condition that can result in user session mix-ups when the appliance is configured as a gateway or AAA virtual server. Both scenarios affect how user identity and session data are processed.

If exploited, an organization could see unauthorized access to internal systems, exposure of sensitive authentication data, or users being placed into the wrong session. This could allow a threat actor to access systems without valid credentials or interact with another user's session. Because these systems often sit at the front of the network, successful exploitation could provide a direct path into internal environments. Aspire recommends patching immediately.

Aspire Protects

- **Patch** - Upgrade to patched versions immediately. See the Citrix advisory for more information.
- Review configurations for:
  - SAML IDP profiles
  - AAA virtual servers
  - VPN or gateway services
- Limit exposure of management and gateway interfaces to the internet where possible.
- Monitor authentication logs for unusual session behavior or anomalies.
- Apply additional access controls such as MFA where applicable.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit vulnerabilities in internet-facing NetScaler devices to gain access to authentication or gateway services.

Credential Access

- Adversary-in-the-Middle [T1557] – The attacker may interfere with authentication or session handling to gain access to user sessions or sensitive identity data.

Behavioral IoCs

- Unusual requests to `/saml/login` or `/wsfed/passive`
- Malformed or incomplete SAMLRequest parameters
- Unexpected responses containing large or encoded data
- Suspicious activity involving the NSC_TASS cookie
- Requests to `/cgi/GetAuthMethods` (recon activity)
- Spikes in authentication-related traffic to NetScaler devices

Targeted Industries

These vulnerabilities impact organizations that rely on Citrix NetScaler for authentication, VPN access, and remote connectivity, especially where these systems are exposed to the internet.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current

security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CITRIX | Support