

Citrix NetScaler Memory Overread Vulnerability

Active Exploitation Observed in the Wild

<https://support.citrix.com/external/article/CTX696300/netscaler-adc-and-netscaler-gateway-secu.html>
 CVEs: CVE-2026-3055

Exploitation activity targeting vulnerable Citrix NetScaler ADC and Gateway appliances remains persistent and widespread, with FortiGuard Labs telemetry continuously observing attack attempts from global sources probing exposed NetScaler SAML endpoints for vulnerable configurations.

Analysis from FortiGuard IPS sensors shows sustained targeting of internet-facing NetScaler deployments configured as SAML Identity Providers (IdP). Attackers continue using malformed authentication requests to exploit the memory overread condition associated with CVE-2026-3055, potentially exposing sensitive session data, authentication tokens, and credential material.

Background

Telemetry collected over the past 30 days (as of the publication date) shows sustained exploitation activity, with FortiGuard IPS sensors frequently detecting over 2,000 blocked CVE-2026-3055 attack attempts per day and peaks exceeding 2,700 daily events. The activity primarily targets exposed NetScaler SAML services across the Technology, Telecom, Automotive, MSSP, and Government sectors, with the highest concentration of attacks observed in Germany, Hong Kong, France, the United States, and Poland.

The vulnerability exists due to insufficient validation of user-supplied parameters during SAML authentication processing. Crafted requests sent to vulnerable SAML endpoints can trigger memory overread conditions, causing portions of process memory to be returned to the attacker.

The vulnerability has received a CVSS v4 score of 9.3 (Critical) and has been added to the Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerabilities (KEV) catalog following confirmed in-the-wild exploitation activity. Most observed activity involves opportunistic scanning and automated exploitation attempts originating from rapidly changing infrastructure, including VPS providers, botnets, and anonymized networks.

Latest Developments

Organizations that have not remediated affected systems remain at risk of credential exposure, account compromise, and unauthorized access to internal resources. The continued volume of observed attacks highlights the elevated risk posed by unpatched or internet-exposed systems, particularly where NetScaler appliances provide federated authentication or remote access services.

- May 25, 2026: CVE-2026-3055 was added to CISA's Known Exploited Vulnerabilities (KEV) catalog.
- March 23, 2026: Public disclosure and security advisories released for CVE-2026-3055, warning of unauthenticated memory disclosure risks affecting NetScaler ADC and Gateway appliances. <https://support.citrix.com/external/article/CTX696300/netscaler-adc-and-netscaler-gateway-secu.html>



PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

IPS

Detects and blocks attack attempts leveraging the vulnerability

 FortiADC DB 36.209	 FortiGate DB 36.209	 FortiNDR DB 36.209	 FortiNDR Cloud DB 36.209	 FortiProxy DB 36.209	 FortiSASE DB 36.209
---------------------------	----------------------------	---------------------------	---------------------------------	-----------------------------	----------------------------

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiWeb


DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

 FortiAnalyzer	 FortiSOCaaS	 FortiSIEM	 FortiSOAR
-------------------	-----------------	---------------	---------------

Outbreak Detection

 FortiAnalyzer DB 2.00095	 FortiSOAR DB 1.0
---------------------------------	-------------------------



RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response


RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
------------------	------------------------

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training


IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Additional Resources

WatchTower Blog <https://labs.watchtower.com/please-we-beg-just-one-weekend-free-of-appliances-citrix-netscaler-cve-2026-3055-memory-overread-part-2/>

Learn more about [FortiGuard Outbreak Alerts](#)