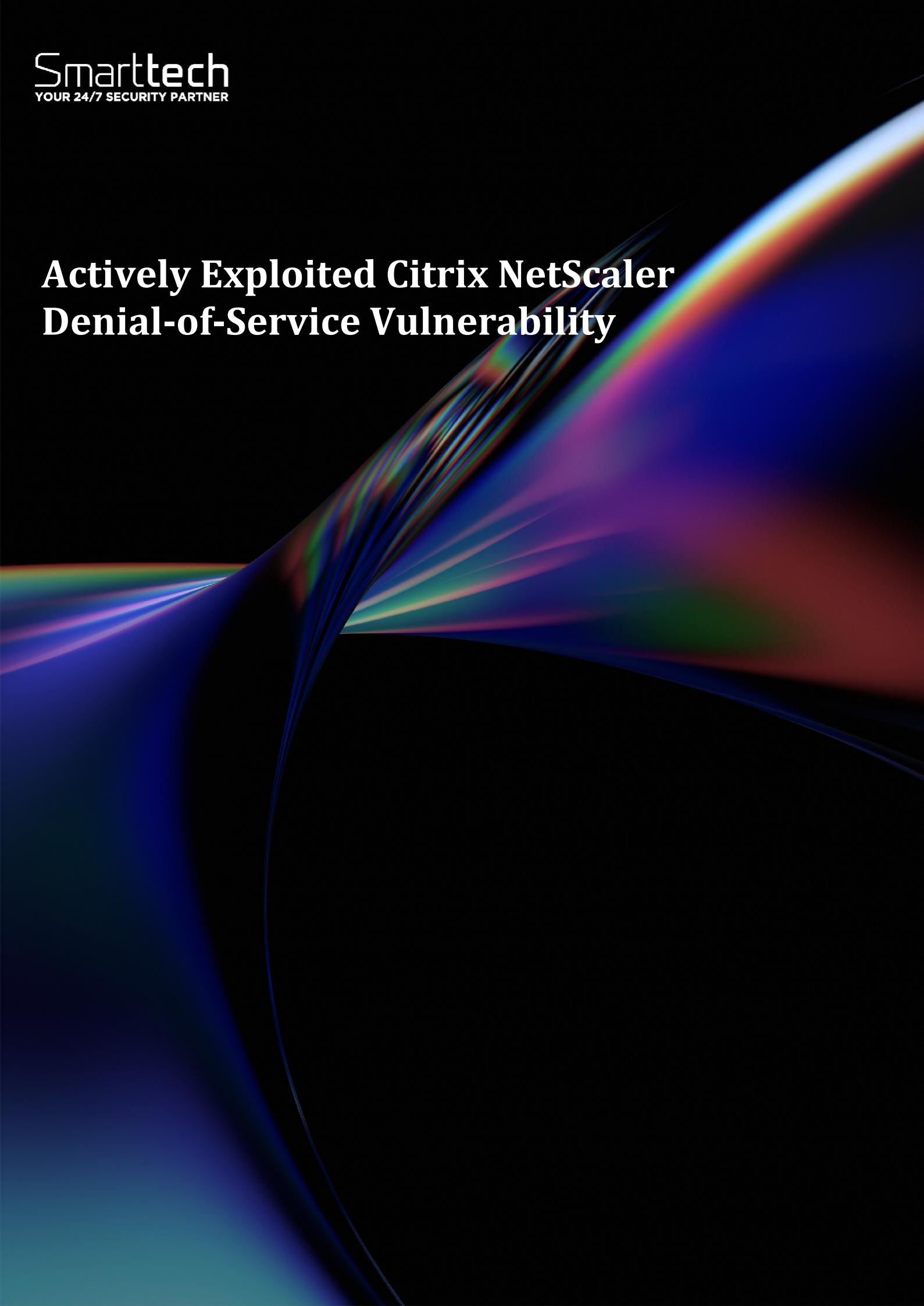
Smarttech
YOUR 24/7 SECURITY PARTNER

Actively Exploited Citrix NetScaler Denial-of-Service Vulnerability



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	174
Authors	Marian Matache < marian.matache@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-05
Issue Date	2026-10-04

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A high severity vulnerability has been discovered in Citrix NetScaler ADC and Citrix NetScaler Gateway that could allow a remote unauthenticated attacker to trigger a memory overflow condition resulting in a Denial of Service. Successful exploitation could impact the availability of affected NetScaler appliances configured as a SAML Service Provider or SAML Identity Provider. NetScaler ADC and NetScaler Gateway are application delivery and secure remote access solutions widely used to provide access to enterprise applications and services.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

TECHNICAL SUMMARY:

More details related to these vulnerabilities are as follows:

CVE ID	***Description***	***Preconditions***
CVE-2026-88779	Memory overflow vulnerability leading to Denial of Service	NetScaler ADC or NetScaler Gateway must be configured as a SAML SP OR SAML IdP

Affected Versions

- Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.41
- Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.28
- Citrix NetScaler ADC FIPS BEFORE 14.1-73.41 FIPS
- Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.282

Customers can determine whether their NetScaler deployment meets the precondition by inspecting their NetScaler configuration for entries matching either of the following:

- Appliance is configured as a SAML SP
  add authentication samlAction

  OR

- Appliance is configured as a SAML IdP
  add authentication samlIdPProfile

Recommendations:

Smarttech247 team recommends the following actions to be taken:

1. **Apply** appropriate updates provided by Citrix to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
   - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
   - **Safeguard 7.2: Establish and Maintain a Remediation Process**: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
   - **Safeguard 7.4**: **Perform Automated Application Patch Management**: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
   - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets**: Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
   - **Safeguard 7.7: Remediate Detected Vulnerabilities**: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
   - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date**: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported

network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program**: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scopes, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests**: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- Safeguard 18.3: Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

2. **Utilize** vulnerability scanning to find potentially exploitable software vulnerabilities to remediate them. (M1016: Vulnerability Scanning)
    - **Safeguard 16.13: Conduct Application Penetration Testing**: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
3. **Apply** the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (M1026: Privileged Account Management)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software**: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts**: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts**: Establish and maintain an inventory of service accounts. The inventory, at a

minimum, must contain the department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- **Safeguard 6.8: Define and Maintain Role-Based Access Control**: Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

4. **Architect** sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (M1030: Network Segmentation)
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
5. **Use** capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050: Exploit Protection)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References:

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174&articleURL=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88779
https://www.cve.org/CVERecord?id=CVE-2026-88779

CVE:

CVE-2026-88779

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com