Citrix Fixes High-Severity NetScaler Console Privilege Escalation Vulnerability

Overview

Citrix has released security updates for a high-severity privilege escalation vulnerability in NetScaler Console (formerly NetScaler ADM) and NetScaler Agent. The flaw, tracked as CVE-2024-12284 (CVSS 8.8), stems from inadequate privilege management, which could allow an authenticated attacker to execute commands without additional authorization.

While only authenticated users with existing access to the NetScaler Console can exploit this vulnerability, organizations should treat this issue with urgency, as it could be leveraged for post-compromise actions.

Affected Products

- NetScaler Console 14.1 before 14.1-38.53
- NetScaler Console 13.1 before 13.1-56.18
- NetScaler Agent 14.1 before 14.1-38.53
- NetScaler Agent 13.1 before 13.1-56.18

There are no workarounds for this vulnerability. Aspire recommends that affected users update to the fixed software versions as soon as possible. Please note that customers using Citrix-managed NetScaler Console Service do not need to take action, as the issue does not affect cloud-managed instances.

Aspire Protects

- **Patch –** Upgrade to the fixed versions listed in Citrix's advisory.
- Implement external authentication – Configure external authentication for NetScaler Console.
- Restrict user access – Limit administrative privileges to essential personnel.

TTPs to Watch

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker may gain elevated privileges through improper access controls.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute unauthorized commands within NetScaler Console.

Persistence

- Create Account [T1136] – The attacker may attempt to create unauthorized accounts for future access.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability affects organizations that rely on NetScaler Console and NetScaler Agent for network management, authentication, and traffic optimization. Industries most at risk include:

- Government
- Energy
- MSPs
- Retail
- Manufacturing
- Telecommunications
- Defense and Aerospace
- Healthcare
- And others

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

NVD - CVE-2025-0893

High-severity security update for NetScaler Console

NetScaler Console and NetScaler Agent Security Bulletin for CVE-2024-12284