Security Advisory 2024-069

Vulnerabilities in Citrix Netscaler

July 15, 2024 — v1.0

TLP:CLEAR

History:

- *15/07/2024 — v1.0 – Initial publication*

Summary

On July 9, 2024, Citrix released a security advisory addressing two vulnerabilities in Citrix NetScaler Console, Agent, and SDX (SVM). The vulnerabilities `CVE-2024-6235` and `CVE-2024-6236` can result in sensitive information disclosure and denial of service [1,2].

Technical Details

The vulnerability `CVE-2024-6235`, with a CVSS score of 9.4 out of 10, can lead to sensitive information disclosure. This vulnerability arises from an improper authentication mechanism in the Citrix NetScaler Console. When exploited, this vulnerability allows an attacker to bypass authentication controls and gain unauthorised access to sensitive information.

The vulnerability `CVE-2024-6236`, with a CVSS score of 7.1 out of 10, can lead to denial of service. This vulnerability is caused by improper restriction of operations within the bounds of a memory buffer.

Affected Products

CVE-2024-6235 affects the following version:

- NetScaler Console 14.1 before 14.1-25.53

CVE-2024-6236 affects the following versions:

- NetScaler Console 14.1 before 14.1-25.53
- NetScaler Console 13.1 before 13.1-53.22
- NetScaler Console 13.0 before 13.0-92.31
- NetScaler SDX (SVM) 14.1 before 14.1-25.53
- NetScaler SDX (SVM) 13.1 before 13.1-53.17
- NetScaler SDX (SVM) 13.0 before 13.0-92.31
- NetScaler Agent 14.1 before 14.1-25.53
- NetScaler Agent 13.1 before 13.1-53.22
- NetScaler Agent 13.0 before 13.0-92.31

Recommendations

CERT-EU strongly recommends updating affected products as soon as possible to mitigate these vulnerabilities.

References

[1] https://support.citrix.com/article/CTX677998/netscaler-console-agent-and-sdx-svm-security-bulletin-for-cve20246235-and-cve20246236

[2] https://cybersecuritynews.com/citrix-netscaler-authentication-vulnerability/