CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-032

Critical CITRIX Vulnerabilities

July 8, 2020 — v1.0

TLP:WHITE

History:

- *08/07/2020 — v1.0 – Initial publication*

Summary

Multiple vulnerabilities have been discovered in Citrix ADC (formerly known as NetScaler ADC), Citrix Gateway (formerly known as NetScaler Gateway) and Citrix SD-WAN WANOP. These vulnerabilities, if exploited, could result in a number of security issues including among others: (i) system compromise by an unauthenticated user on the management network, (ii) system compromise through Cross Site Scripting (XSS) on the management interface, (iii) denial of service against either the Gateway or Authentication virtual servers by an unauthenticated user [1].

Technical Details

The Citrix Security Bulletin lists 11 vulnerabilities in total. The details of the vulnerabilities and prerequisites to exploit them are provided in [1]. In particular, for attacks that are limited to the management interface pose the following security issues:

- System compromise by an unauthenticated user on the management network.
- System compromise through Cross Site Scripting (XSS) on the management interface
- Creation of a download link for the device which, if downloaded and then executed by an unauthenticated user on the management network, may result in the compromise of their local computer.

Mitigating Factors: Customers who have configured their systems in accordance with Citrix recommendations in [3], have significantly reduced their risk from attacks to the management interface.

For attacks that are applicable to a Virtual IP (VIP), the security issues include:

- Denial of service against either the Gateway or Authentication virtual servers by an unauthenticated user (the load balancing virtual server is unaffected).
- Remote port scanning of the internal network by an authenticated Citrix Gateway user. Attackers can only discern whether a TLS connection is possible with the port and cannot communicate further with the end devices.

Mitigating Factors: Customers who have not enabled either the Gateway or Authentication virtual servers are not at risk from attacks that are applicable to those servers. Other virtual servers e.g. load balancing and content switching virtual servers are not affected by these issues.

Products Affected

- Citrix ADC (formerly known as NetScaler ADC),
- Citrix Gateway (formerly known as NetScaler Gateway),
- Citrix SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO

Recommendations

The following versions of Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP remediate the vulnerabilities [1]:

- Citrix ADC and Citrix Gateway 13.0-58.30 and later releases
- Citrix ADC and NetScaler Gateway 12.1-57.18 and later 12.1 releases
- Citrix ADC and NetScaler Gateway 12.0-63.21 and later 12.0 releases
- Citrix ADC and NetScaler Gateway 11.1-64.14 and later 11.1 releases
- NetScaler ADC and NetScaler Gateway 10.5-70.18 and later 10.5 releases
- Citrix SD-WAN WANOP 11.1.1a and later releases
- Citrix SD-WAN WANOP 11.0.3d and later 11.0 releases
- Citrix SD-WAN WANOP 10.2.7 and later 10.2 releases
- Citrix Gateway Plug-in for Linux 1.0.0.137 and later versions

References

[1] https://support.citrix.com/article/CTX276688

[2] https://www.citrix.com/blogs/2020/07/07/citrix-provides-context-on-security-bulletin-ctx276688/

[3] https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html