Security Advisory 2020-002

Critical Vulnerability in Citrix Products

*February 3, 2020 — v1.6*

TLP:WHITE

History:

- 13/01/2020 — v1.0 – Initial publication
- 14/01/2020 — v1.1 – Updated with risks associated with common Cloud Services
- 15/01/2020 — v1.2 – Updated with guidelines for investigating affected systems
- 16/01/2020 — v1.3 – Updated with additional affected products and versions
- 20/01/2020 — v1.4 – Updated with information about some patches available
- 24/01/2020 — v1.5 – Updated with additional detection tools and more patches available
- 03/03/2020 — v1.6 – Updated with additional investigation guidelines

Summary

A critical vulnerability affecting Citrix products has been disclosed in December 2019 [1]. The vulnerability, identified as CVE-2019-19781, could allow an attacker to get access to the internal network without requiring authentication. Numerous exploits to leverage this vulnerability have been publicly released [6, 7, 8]. As of 24/01/2020 all patches are available, but an investigation of potential compromises is advised.

Technical Details

The affected Citrix products fail to restrict access to Perl scripts using directory traversal [2]. A remote attacker could provide crafted contents to these scripts without being authenticated. This results in an arbitrary code execution [5].

Products Affected

This vulnerability affects the following products [5]:

- Citrix ADC and Citrix Gateway version 13.0 all supported builds
- Citrix ADC and NetScaler Gateway version 12.1 all supported builds
- Citrix ADC and NetScaler Gateway version 12.0 all supported builds
- Citrix ADC and NetScaler Gateway version 11.1 all supported builds
- Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds
- Citrix SD-WAN WANOP software and appliance models 4000, 4100, 5000, and 5100 all supported builds
Recommendations

Permanent fixes for the affected products are now available [11, 13]. It is recommended to patch as soon as possible. These fixes also apply to Citrix ADC and Citrix Gateway Virtual Appliances (VPX) hosted on any of ESX, Hyper-V, KVM, XenServer, Azure, AWS, GCP or on a Citrix ADC Service Delivery Appliance (SDX). SVM on SDX does not need to be updated [11]. In addition, it is advised to change the default root password of these appliances as it seems to be easily retrievable [9].

Where patching is not possible, Citrix has provided some steps to mitigate the problem [4, 5, 6]. It is highly recommended to mitigate this vulnerability followings the steps provided by Citrix, and then patch as soon as possible.

When investigating potential compromised Citrix installation, the CVE-2019-19781 DFIR Notes in [10] may be used as a guideline. Also, FireEye has published a scanner that can help in detecting compromised systems [12, 13]. Additionally, US-CERT has also published an investigation guidelines that should help in detecting potential compromises that could have happened before the mitigations or patches were applied [14].

References

[4] https://support.citrix.com/user/alerts
[9] https://twitter.com/KevTheHermit/status/1216318333219491840