CTX267027

CVE-2019-19781 -Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance

Security Bulletin | Critical | 170 found this helpful | Created: 16 Dec 2019 | Modified: 22 Oct 2020

Applicable Products

NetScaler NetScaler Gateway Citrix ADC Citrix Gateway Citrix SD-WAN WANOP

Description of Problem

A vulnerability has been identified in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution.

The scope of this vulnerability includes Citrix ADC and Citrix Gateway Virtual Appliances (VPX) hosted on any of Citrix Hypervisor (formerly XenServer), ESX, Hyper-V, KVM, Azure, AWS, GCP, Citrix ADC MPX or Citrix ADC SDX.

Further investigation by Citrix has shown that this issue also affects certain deployments of Citrix SD-WAN, specifically Citrix SD-WAN WANOP edition. Citrix SD-WAN WANOP edition packages Citrix ADC as a load balancer thus resulting in the affected status.

The vulnerability has been assigned the following CVE number:

• CVE-2019-19781 : Vulnerability in Citrix Application Delivery Controller, Citrix Gateway and Citrix SD-WAN WANOP appliance leading to arbitrary code execution

The vulnerability affects the following supported product versions on all supported platforms:

• Citrix ADC and Citrix Gateway version 13.0 all supported builds before 13.0.47.24

• NetScaler ADC and NetScaler Gateway version 12.1 all supported builds before 12.1.55.18

• NetScaler ADC and NetScaler Gateway version 12.0 all supported builds before 12.0.63.13

• NetScaler ADC and NetScaler Gateway version 11.1 all supported builds before 11.1.63.15

• NetScaler ADC and NetScaler Gateway version 10.5 all supported builds before 10.5.70.12

• Citrix SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO all supported software release builds before 10.2.6b and 11.0.3b

What Customers Should Do

Exploits of this issue on unmitigated appliances have been observed in the wild. Citrix strongly urges affected customers to immediately upgrade to a fixed build OR apply the provided mitigation which applies equally to Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP deployments. Customers who have chosen to immediately apply the mitigation should then upgrade all of their vulnerable appliances to a fixed build of the appliance at their earliest schedule. Subscribe to bulletin alerts at https://support.citrix.com/user/alerts to be notified when the new fixes are available.

The following knowledge base article contains the steps to deploy a responder policy to mitigate the issue in the interim until the system has been updated to a fixed build: CTX267679 - Mitigation steps for CVE-2019-19781

Upon application of the mitigation steps, customers may then verify correctness using the tool published here: CTX269180 - CVE-2019-19781 – Verification Tool

In Citrix ADC and Citrix Gateway Release "12.1 build 50.28", an issue exists that affects responder and rewrite policies causing them not to process the packets that matched policy rules. This issue was resolved in "12.1 build 50.28/31" after which the mitigation steps, if applied, will be effective. However, Citrix recommends that customers using these builds now update to "12.1 build 55.18", or later, where CVE-2019-19781 issue is already addressed.

Customers on "12.1 build 50.28" who wish to defer updating to "12.1 build 55.18" or later should choose one from the following two options for the mitigation steps to function as intended:

1. Update to the refreshed "12.1 build 50.28/50.31" or later and apply the mitigation steps, OR

2. Apply the mitigation steps towards protecting the management interface as published in CTX267679. This will mitigate attacks, not just on the management interface but on ALL interfaces including Gateway and AAA virtual IPs

Fixed builds have been released across all supported versions of Citrix ADC and Citrix Gateway. Fixed builds have also been released for Citrix SD-WAN WANOP for the applicable appliance models. Citrix strongly recommends that customers install these updates at their earliest schedule. The fixed builds can be downloaded from https://www.citrix.com/downloads/citrix-adc/ and https://www.citrix.com/downloads/citrix-gateway/ and https://www.citrix.com/downloads/citrix-sd-wan/

Customers who have upgraded to fixed builds do not need to retain the mitigation described in CTX267679.

Fix Timelines

Citrix has released fixes in the form of refresh builds across all supported versions of Citrix ADC, Citrix Gateway, and applicable appliance models of Citrix SD-WAN WANOP. Please refer to the table below for the release dates.

Citrix ADC and Citrix Gateway		
Version	Refresh Build	Release Date
10.5	10.5.70.12	24th January 2020 (Released)
11.1	11.1.63.15	19th January 2020 (Released)
12.0	12.0.63.13	19th January 2020 (Released)
12.1	12.1.55.18	23rd January 2020 (Released)
13.0	13.0.47.24	23rd January 2020 (Released)
Citrix SD-WAN WANOP		
Release	Citrix ADC Release	Release Date
10.2.6b	11.1.51.615	22nd January 2020 (Released)
11.0.3b	11.1.51.615	22nd January 2020 (Released)

Acknowledgements

Citrix thanks Mikhail Klyuchnikov of Positive Technologies, and Gianlorenzo Cipparrone and Miguel Gonzalez of Paddy Power Betfair plc for working with us to protect Citrix customers.

What Citrix Is Doing

Citrix is notifying customers and channel partners about this potential security issue. This article is also available from the Citrix Knowledge Center at http://support.citrix.com/.

Obtaining Support on This Issue

If you require technical assistance with this issue, please contact Citrix Technical Support. Contact details for Citrix Technical Support are available at https://www.citrix.com/support/open-a-support-case.html.

Reporting Security Vulnerabilities

Citrix welcomes input regarding the security of its products and considers any and all potential vulnerabilities seriously. For guidance on how to report security-related issues to Citrix, please see the following document: CTX081743 – Reporting Security Issues to Citrix

Changelog

Date	Change
17th December 2019	Initial Publication
11th January 2020	Fix Timelines Updated
16th January 2020	SD-WAN WANOP added/Citrix ADC 12.1 responder bug detail added
16th January 2020	CVE verification tool
17th January 2020	Update to Citrix ADC and Citrix Gateway 12.1 responder policy issue

Was this page helpful? Please provide article feedback.

Featured Products

Digital Workspaces

Citrix Virtual Apps and Desktops

Citrix Workspace App | StoreFront

Citrix App Layering | Citrix Hypervisor

Citrix Endpoint Management | ShareFile

Citrix Content Collaboration

Networking

Citrix ADC

Citrix Application Delivery Management

Citrix Gateway | Citrix SD-WAN

Need more help?

PRODUCT ISSUES

Open a case

Chat live

LICENSING, RENEWAL, OR GENERAL ACCOUNT ISSUES

Select a region Go

OTHER SUPPORT OPTIONS

Citrix Product Documentation

Citrix Discussions

View Support numbers

SHARE THIS PAGE

● ● ● ●

citrix

Privacy & Terms | Cookie Preferences