Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance Security Update

Title
Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance Security Update

CTX Number
CTX276688

Article Type
Security Bulletin

Created Date
9/Nov/2020

Last Modified Date
14/Nov/2020

Severity
Critical

Solution

Description of Problem

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 appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO. These vulnerabilities, if exploited, could result in a number of security issues including:

Attacks that are limited to the management interface

- 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 https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html have significantly reduced their risk from attacks to the management interface.

Attacks that are applicable to a Virtual IP (VIP)

- 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.

In addition, a vulnerability has been found in Citrix Gateway Plug-in for Linux that would allow a local logged-on user of a Linux system with that plug-in installed to elevate their privileges to an administrator account on that computer.

The issues have the following identifiers:

CVE ID	Vulnerability Type	Affected Products	Attacker privileges	Pre-conditions
CVE-2019-18177	Information disclosure	Citrix ADC, Citrix Gateway	Authenticated VPN user	Requires a configured SSL VPN endpoint
CVE-2020-8187	Denial of service	Citrix ADC, Citrix Gateway 12.0 and 11.1 only	Unauthenticated remote user	Requires a configured SSL VPN or AAA endpoint
CVE-2020-8190	Local elevation of privileges	Citrix ADC, Citrix Gateway	Authenticated user on the NSIP	This issue cannot be exploited directly. An attacker must first obtain nobody privileges using another exploit
CVE-2020-8191	Reflected Cross Site Scripting (XSS)	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Unauthenticated remote user	Requires a victim who must open an attacker-controlled link in the browser whilst being on a network with connectivity to the NSIP
CVE-2020-8193	Authorization bypass	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Unauthenticated user with access to the NSIP	Attacker must be able to access the NSIP
CVE-2020-8194	Code Injection	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Unauthenticated remote user	Requires a victim who must download and execute a malicious binary from the NSIP
CVE-2020-8195	Information disclosure	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Authenticated user on the NSIP	-
CVE-2020-8196	Information disclosure	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Authenticated user on the NSIP	-
CVE-2020-8197	Elevation of privileges	Citrix ADC, Citrix Gateway	Authenticated user on the NSIP	-
CVE-2020-8198	Stored Cross Site Scripting (XSS)	Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP	Unauthenticated remote user	Requires a victim who must be logged in as an administrator (nsroot) on the NSIP
CVE-2020-8199	Local elevation of privileges	Citrix Gateway Plug-in for Linux	Local user on the Linux computer running Citrix Gateway Plug-in	A pre-installed version of Citrix Gateway Plug-in for Linux must be running

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

- 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 ADC FIPS 12.1-55.179 and later 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

What Customers Should Do

Fixed builds have been released for all supported versions of Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP. Citrix strongly recommends that customers immediately install these updates.

The latest 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 are unable to immediately update to the latest version are advised ensure access to the management interface is restricted. Please see https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html for more information.

Users with Citrix Gateway Plug-in for Linux should log-in to an updated version of Citrix Gateway and select 'Network VPN mode'. Citrix Gateway will then prompt the user to update.

Customers with Citrix-managed Citrix Gateway service do not need to take any action.

Acknowledgements

Citrix thanks Laurent Geyer of Akamai, Muris Kurgas of Digital 14 (Xen1thLabs), Maarten Boone (@staatsgeheim), Donny Maasland (@donnymaasland), Albert Shi of Univision Network (Shanghai) Co., Ltd and Viktor Dragomiretskyy 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 details on our vulnerability response process and guidance on how to report security-related issues to Citrix, please visit the Citrix Trust Center at https://www.citrix.com/about/trust-center/vulnerability-process.html .

Changelog

Date	Change
2020-07-07	Initial publication
2020-08-17	Added FIPS Build

NetScaler | Netscaler Gateway | Citrix SD-WAN WANOP