CYBERSECURITY ADVISORY

Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Last Revised: May 21, 2020 **Alert Code:** AA20-020A

Summary

Note: As of January 24, 2020, Citrix has released all expected updates in response to CVE-2019-19781.[1] <https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/>

On January 19, 2020, Citrix released firmware updates for Citrix Application Delivery Controller (ADC) and Citrix Gateway versions 11.1 and 12.0.

On January 22, 2020, Citrix released security updates for vulnerable SD-WAN WANOP appliances.

On January 23, 2020, Citrix released firmware updates for Citrix ADC and Gateway versions 12.1 and 13.0.

On January 24, 2020, Citrix released firmware updates for Citrix ADC and Gateway version 10.5.

A remote, unauthenticated attacker could exploit CVE-2019-19781 to perform arbitrary code execution.[2] <https://support.citrix.com/article/ctx267027> This vulnerability has been detected in exploits in the wild.[3] <https://www.ncsc.gov.uk/news/citrix-alert>

The Cybersecurity and Infrastructure Agency (CISA) strongly recommends that all users and administrators upgrade their vulnerable appliances as soon as possible.

Timeline of Specific Events

- December 17, 2019 – Citrix released Security Bulletin CTX267027 with mitigations steps.
- January 8, 2020 – The CERT Coordination Center (CERT/CC) released Vulnerability Note VU#619785: Citrix Application Delivery Controller and Citrix Gateway Web Server Vulnerability,[4] <https://www.kb.cert.org/vuls/id/619785/> and CISA releases a Current Activi entry.[5] <https://www.us-cert.gov/ncas/current-activity/2020/01/08/citrix-application-delivery-controller-and-citrix-gateway>
- January 10, 2020 – The National Security Agency (NSA) released a Cybersecurity Advisory on CVE-2019-19781.[6] <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf>
- January 11, 2020 – Citrix released blog post on CVE-2019-19781 with timeline for fixes. [7] <https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/>

- January 13, 2020 – CISA released a Current Activity entry describing their utility that enables users and administrators to test whether their Citrix ADC and Citrix Gateway firmware is susceptible to the CVE-2019-19781 vulnerability.[8] <https://www.us-cert.gov/ncas/current-activity/2020/01/13/cisa-releases-test-citrix-adc-and-gateway-vulnerability>
- January 16, 2020 – Citrix announced that Citrix SD-WAN WANOP appliance is also vulnerable to CVE-2019-19781.
- January 19, 2020 – Citrix released firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 and blog post on accelerated schedule for fixes.[9] <https://www.citrix.com/blogs/2020/01/19/vulnerability-update-first-permanent-fixes-available-timeline-accelerated/>
- January 22, 2020 – Citrix released security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3.[10] <https://www.citrix.com/blogs/2020/01/22/update-on-cve-2019-19781-fixes-now-available-for-citrix-sd-wan-wanop/>
- January 22, 2020 – Citrix and FireEye Mandiant released an indicator of compromise (IOC) scanning tool for CVE-2019-19781.[11] <https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/>
- January 23, 2020 – Citrix released firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0.[12] <https://www.citrix.com/blogs/2020/01/23/fixes-now-available-for-citrix-adc-citrix-gateway-versions-12-1-and-13-0/>
- January 24, 2020 – Citrix released firmware updates for Citrix ADC and Citrix Gateway version 10.5.

Technical Details

Impact

On December 17, 2019, Citrix reported vulnerability CVE-2019-19781. A remote, unauthenticated attacker could exploit this vulnerability to perform arbitrary code execution. This vulnerability has been detected in exploits in the wild.

The vulnerability affects the following appliances:

- Citrix NetScaler ADC and NetScaler Gateway version 10.5 – all supported builds before 10.5.70.12
- Citrix ADC and NetScaler Gateway version 11.1 – all supported builds before 11.1.63.15
- Citrix ADC and NetScaler Gateway version 12.0 – all supported builds before 12.0.63.13
- Citrix ADC and NetScaler Gateway version 12.1 – all supported builds before 12.1.55.18
- Citrix ADC and Citrix Gateway version 13.0 – all supported builds before 13.0.47.24
- 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. (Citrix SD-WAN WANOP is vulnerable because it packages Citrix ADC as a load balancer).

Detection Measures

Citrix and FireEye Mandiant released an IOC scanning tool for CVE-2019-19781 <https://github.com/citrix/ioc-scanner-cve-2019-19781/> on January 22, 2020. The tool aids customers with detecting potential IOCs based on known attacks and exploits.[13] <https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/>

See the National Security Agency's Cybersecurity Advisory on CVE-2019-19781 for other detection measures.[14] <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_2020 09.pdf>

CISA released a utility that enables users and administrators to detect whether their Citrix ADC and Citrix Gateway firmware is susceptible to CVE-2019-19781.[15] <https://www.us-cert.gov/ncas/current-activity/2020/01/13/cisa-releases-test-citrix-adc-and-gateway-vulnerability>CISA encourages administrators to visit CISA's GitHub page <https://github.com/cisagov/check-cve-2019-19781> to download and run the tool.

Mitigations

CISA strongly recommends users and administrators update Citrix ADC, Citrix Gateway, and Citrix SD-WAN WANOP as soon as possible.

The fixed builds can be downloaded from Citrix Downloads pages for Citrix ADC <https://www.citrix.com/downloads/citrix-adc/>, Citrix Gateway <https://www.citrix.com/downloads/citrix-gateway/>, and Citrix SD-WAN <https://www.citrix.com/downloads/citrix-sd-wan/>.

Until the appropriate update is implemented, users and administrators should apply Citrix's interim mitigation steps for CVE-2019-19781.[16] <https://support.citrix.com/article/ctx267679> Verify the successful application of the above mitigations by using the tool in CTX269180 – CVE-2019-19781 – Verification ToolTest <https://support.citrix.com/article/ctx269180>. **Note:** these mitigation steps apply to Citrix ADC and SD-WAN WANOP deployments.[17] <https://support.citrix.com/article/ctx267027>

Refer to table 1 for Citrix's fix schedule.[18] <https://support.citrix.com/article/ctx267027>

Table 1. Fix schedule for Citrix appliances vulnerable to CVE-2019-19781

Vulnerable Appliance	Firmware Update	Release Date
Citrix ADC and Citrix Gateway version 10.5	Refresh Build 10.5.70.12	January 24, 2020
Citrix ADC and Citrix Gateway version 11.1	Refresh Build 11.1.63.15	January 19, 2020
Citrix ADC and Citrix Gateway version 12.0	Refresh Build 12.0.63.13	January 19, 2020
Citrix ADC and Citrix Gateway version 12.1	Refresh Build 12.1.55.18	January 23, 2020
Citrix ADC and Citrix Gateway version 13.0	Refresh Build 13.0.47.24	January 23, 2020
Citrix SD-WAN WANOP Release 10.2.6	Build 10.2.6b	January 22, 2020
Citrix SD-WAN WANOP Release 11.0.3	Build 11.0.3b	January 22, 2020

Administrators should review NSA's Citrix Advisory <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf> for other mitigations, such as applying the following defense-in-depth strategy:

"Consider deploying a VPN capability using standardized protocols, preferably ones listed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL), in front of publicly accessible Citrix ADC and Citrix Gateway appliances to require user

authentication for the VPN before being able to reach these appliances. Use of a proprietary SSLVPN/TLSVPN is discouraged."

References

[1] Citrix blog: Citrix releases final fixes for CVE-2019-19781 <https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/>

[2] Citrix Security Bulletin CTX267027, Vulnerability in Citrix Application Delivery Controller and Citrix Gateway <https://support.citrix.com/article/ctx267027>

[3] United Kingdom National Cyber Secrity Centre (NCSC) Alert: Actors exploiting Citrix products vulnerability <https://www.ncsc.gov.uk/news/citrix-alert>

[4] CERT/CC Vulnerability Note VU#619785 <https://www.kb.cert.org/vuls/id/619785/>

[5] CISA Current Activity: Citrix Application Delivery Controller and Citrix Gateway Vulnerability <https://www.us-cert.gov/ncas/current-activity/2020/01/08/citrix-application-delivery-controller-and-citrix-gateway>

[6] NSA Cybersecurity Advisory: Mitigate CVE-2019-19781: Critical Vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf>

[7] Citrix blog: Citrix provides update on Citrix ADC, Citrix Gateway vulnerability <https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/>

[8] CISA Current Activity: CISA Releases Test for Citrix ADC and Gateway Vulnerability GitHub: CISAgov – check-cve-2019-19781 <https://www.us-cert.gov/ncas/current-activity/2020/01/13/cisa-releases-test-citrix-adc-and-gateway-vulnerability>

[9] Citrix Blog: Vulnerability Update: First permanent fixes available, timeline accelerated <https://www.citrix.com/blogs/2020/01/19/vulnerability-update-first-permanent-fixes-available-timeline-accelerated/>

[10] Citrix Blog: Update on CVE-2019-19781: Fixes now available for Citrix SD-WAN WANOP <https://www.citrix.com/blogs/2020/01/22/update-on-cve-2019-19781-fixes-now-available-for-citrix-sd-wan-wanop/>

[11] Citrix Blog: Citrix and FireEye Mandiant share forensic tool for CVE-2019-19781 <https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/>

[12] Citrix Blog: Fixes now available for Citrix ADC, Citrix Gateway versions 12.1 and 13.0 <https://www.citrix.com/blogs/2020/01/23/fixes-now-available-for-citrix-adc-citrix-gateway-versions-12-1-and-13-0/>

[13] Citrix Blog: Citrix and FireEye Mandiant share forensic tool for CVE-2019-19781 <https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/>
[14] NSA Cybersecurity Advisory: Mitigate CVE-2019-19781: Critical Vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway <https://media.defense.gov/2020/jan/10/2002233132/-1/-1/0/csa%20for%20citrixadcandcitrixgateway_20200109.pdf>
[15] CISA Current Activity: CISA Releases Test for Citrix ADC and Gateway Vulnerability GitHub: CISAgov – check-cve-2019-19781 <https://www.us-cert.gov/ncas/current-activity/2020/01/13/cisa-releases-test-citrix-adc-and-gateway-vulnerability>
[16] Citrix Security Bulletin CTX267679, Mitigation Steps for CVE-2019-19781 <https://support.citrix.com/article/ctx267679>
[17] Citrix Security Bulletin CTX267027, Vulnerability in Citrix Application Delivery Controller and Citrix Gateway <https://support.citrix.com/article/ctx267027>
[18] Citrix Security Bulletin CTX267027, Vulnerability in Citrix Application Delivery Controller and Citrix Gateway <https://support.citrix.com/article/ctx267027>

Revisions

January 20, 2020: Initial Version|January 23, 2020: Updated with information about Citrix releasing fixes for SD-WAN WANOP appliances and an IOC scanning tool|January 24, 2020: Updated with information about Citrix releasing fixes for Citrix ADC and Gateway versions 10.5, 12.1, and 13.0|January 27, 2020: Updated vulnernable versions of ADC and Gateway version 10.5

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov