NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

MITIGATE CVE-2019-19781:

CRITICAL VULNERABILITY IN CITRIX APPLICATION DELIVERY CONTROLLER (ADC) AND CITRIX GATEWAY

DISCUSSION

On December 17, 2019, Citrix®[1] published an advisory for a critical vulnerability (CVE-2019-19781) in Citrix Application Delivery Controller (Citrix ADC™[1]/NetScaler ADC™[1]) and Citrix Gateway™[1] (NetScaler Gateway™[1]).[2] [3] If unmitigated, adversaries could exploit this vulnerability to gain remote code execution on affected appliances without credentials, potentially enabling access to other internal resources and sensitive data.[2] Citrix also released an interim mitigation for the vulnerability.[4] Citrix Virtual Apps and Desktops™[1] users typically access their applications and desktops through Citrix ADC or Citrix Gateway appliances that are frequently deployed in front of Citrix Virtual Desktop Infrastructure (VDI) products and web applications. The appliances are often accessible from the Internet to allow remote connections, increasing their risk of exploitation.

Security researchers have reproduced an exploit for this vulnerability and have detected scanning for vulnerable appliances and exploitation attempts in the wild.[5] [6] [7]

MITIGATION ACTIONS

Apply the Citrix published interim mitigation for CVE-2019-19781 immediately.

The Citrix mitigation can be found at https://support.citrix.com/article/CTX267679.[4] All supported builds of Citrix ADC (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) version 13.0, 12.1, 12.0, 11.1, and 10.5 are vulnerable.[2] Although a patched firmware update is not available, the Citrix mitigation will help prevent exploitation while patches are developed. Procedures should be in place to apply mitigations, patches, and updates in a timely manner.

Update Citrix ADC and Citrix Gateway to patched firmware once Citrix releases a patch.[2]

Running the most up-to-date patched version reduces risk of successful exploitation.

Apply defense-in-depth security 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.

---

[1] Citrix, Citrix ADC, NetScaler ADC, Citrix Gateway, NetScaler Gateway, Citrix Virtual Apps and Desktops are registered trademarks of Citrix System, Inc.

[2] https://support.citrix.com/article/CTX267027

[3] https://nvd.nist.gov/vuln/detail/CVE-2019-19781

[4] https://support.citrix.com/article/CTX267679

[5] https://tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/

[6] https://isc.sans.edu/forums/diary/Some+Thoughts+About+the+Critical+Citrix+ADCGateway+Vulnerability+CVE201919781/25660/

[7] https://isc.sans.edu/forums/diary/A+Quick+Update+on+Scanning+for+CVE201919781+Citrix+ADC+Gateway+Vulnerability/25686/

If a web application firewall (WAF) or an intrusion detection system (IDS) with TLS Inspection (break and inspect) is deployed to protect these appliances, apply the following rules:

- For non-SSL VPN configurations, send a HTTP 403 response for requests containing "/vpns/"[6]
- For SSL VPN enabled configurations, send a HTTP 403 response for:
  - requests containing both "/vpns/" with "/../"[6]
  - requests containing "/vpns/cfg/smb.conf"[7]

Detecting potential exploitation attempts.

- For non-SSL VPN configurations, review the web request logs for requests containing "/vpns/"[6]
- For SSL VPN enabled configurations, review the web request logs. There will be legitimate requests containing "/vpns/", but potentially malicious web requests include at least:
  - requests containing both "/vpns/" and "/../"[6]
  - requests containing "/vpns/cfg/smb.conf"[7]

Responding to potential exploitation attempts.

- If the detection rules described above trigger an alert, review the web request logs for unusual requests (see above).
- If warranted, perform a forensic triage of the appliance for potential signs of compromise (e.g., unusual additional files or file modifications, unusual processes, additional accounts, or account modifications).
- If there are signs of appliance compromise, perform incident response assuming lateral movement has occurred.

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or endorsement purposes.

NOTICE

The information contained in this document was developed in the course of NSA's cybersecurity missions including its responsibilities to identify and disseminate threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

CONTACT

For general cybersecurity inquiries and reporting, contact the

NSA Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov.

For media inquiries, contact the

NSA Press Desk, 443-634-0721, MediaRelations@nsa.gov.