HC3: Sector Alert
December 16, 2022 TLP:CLEAR Report: 202212161700

Citrix ADC and Gateway Vulnerabilities

Executive Summary
Citrix released patches for a vulnerability that impacts both their Application Delivery Controller and Gateway platforms. This vulnerability allows a remote attacker to completely compromise a target system. These vulnerabilities are known to be actively exploited by a highly capable state-sponsored adversary. Furthermore, the Department of Health and Human Services is aware of U.S. healthcare entities that have already been compromised by the exploitation of this vulnerability. HC3 strongly urges all healthcare and public health organizations to review their inventory for these systems and prioritize the implementation of these patches.

Report
Citrix has recently patched what they describe as a "critical" zero-day vulnerability in their Application Delivery Controller and Gateway. This vulnerability, which is actively compromised, allows an unauthenticated attacker to potentially execute commands remotely on vulnerable devices and completely compromise a system. This report contains the steps necessary to completely protect a system from potential compromise.

Report
These vulnerabilities are known to be actively exploited by a Chinese state-sponsored advanced persistent threat known as APT5, and also UNC2630 and MANGANESE. Separately, the US Department of Health and Human Services is aware of U.S. healthcare organizations that have already been compromised by the exploitation of the vulnerability described in this report, although in each case the specific attacker has not yet been identified.

Vulnerability
This vulnerability is tracked as CVE-2022-27518 and impacts the following versions of Citrix ADC and Citrix Gateway:

- Citrix ADC and Citrix Gateway 13.0 before 13.0-58.32
- Citrix ADC and Citrix Gateway 12.1 before 12.1-65.25
- Citrix ADC 12.1-FIPS before 12.1-55.291
- Citrix ADC 12.1-NDcPP before 12.1-55.291 nec lorem

Furthermore, any of the affected versions of the two platforms must be configured as a SAML (Security Assertion Markup Language) service provider or identity provider. As per Citrix guidance, customers can determine if their Citrix ADC or Citrix Gateway is configured as a SAML SP or a SAML IdP by inspecting the "ns.conf" file for the following commands:

- "add authentication samlAction"
- "add authentication samlIdPProfile"

Either one of these commands being present in the "ns.conf" file (on an instance of one of the affected platform versions listed above) is an indication that the system in question is vulnerable.

HC3: Sector Alert
December 16, 2022 TLP:CLEAR Report: 202212161700

Patches, Mitigations, and Workarounds

The most optimal solution is to upgrade all vulnerable instances of these Citrix platforms. For any organization running YARA, there are signatures available.

Upon detection of compromise of these vulnerabilities, the following actions are recommended by the National Security Agency:

- Move all Citrix ADC instances behind a VPN or other capability that requires valid user authentication (ideally multi-factor) prior to being able to access the ADC.
- Isolate the Citrix ADC appliances from the environment to ensure any malicious activity is contained.
- Restore the Citrix ADC to a known good state

References

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2022-27518
https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518

Critical security update now available for Citrix ADC, Citrix Gateway
https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/

APT5: Citrix ADC Threat Hunting Guidance
https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF

State-sponsored attackers actively exploiting RCE in Citrix devices, patch ASAP! (CVE-2022-27518)
https://www.helpnetsecurity.com/2022/12/13/cve-2022-27518-exploited/

Hackers exploit critical Citrix ADC and Gateway zero day, patch now
https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-citrix-adc-and-gateway-zero-day-patch-now/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback