WHITE PAPER | APT41 Citrix and Zoho Attacks on Healthcare

March 26, 2020 **TLP: WHITE**

Health Sector Cybersecurity Coordination Center (HC3) | HC3@HHS.GOV

Executive Summary

A recent campaign of cyberattacks from a foreign threat actor targeted healthcare organizations and specifically exploited Citrix and Zoho technologies used for remote desktop services among others. These attacks allow attackers the ability to conduct reconnaissance and execute code on the victim systems and access to corporate networks. Patches have been released for both vulnerabilities and should be implemented as soon as possible.

Overview of the Exploit

An Advanced Persistent Threat is a threat actor, often representative of a nation state, that attempts to gain and maintain access to victim systems for extended periods of time while conducting further cyber-attacks. APT41, a Chinese cyber threat actor historically known to target the healthcare industry among others, was recently observed to exploit vulnerable technologies, such as Citrix and Zoho endpoints, as part of a recent wide-reaching global campaign (Clyer, et. al., 2020 and Muncaster, 2020). Recently, several United States organizations were targeted with attacks attributed to APT41, including those in the healthcare sector. Two critical vulnerabilities were used in these attacks, CVE-2019-19781 and CVE-2020-10189 (Muncaster, 2020).

- When exploited, the Citrix vulnerability (CVE-2019-19781) allows for directory traversal of a system, giving an attacker access to areas of a victim system they would not otherwise have. Such an attack may allow for the theft of sensitive information, but also to prepare the system for a future attack stage (NVD #1, 2020 and Citrix, 2020).
- When exploited, the Zoho vulnerability (CVE-2020-10189) allows for remote code execution (RCE). RCE vulnerabilities may allow an attacker to deliver additional malware to maintain persistent access, conduct reconnaissance, or produce other malicious effects (NVD #2, 2020 and SourceIncite, 2020).

APT41 is known to conduct 'off-duty' cyber operations, likely for the direct personal benefit of its individual members, motivated by financial gain, rather than for the sake of the Chinese Government (Lyngass, 2019). Given its criticality to our communities, perceived availability of financial resources and highly valuable quantities of protected health information (PHI), and relatively unprepared IT infrastructures, the healthcare industry is historically susceptible to ransomware attacks; an appealing target to APT41.

Countermeasures and Mitigations

The Health Sector Cybersecurity Coordination Center (HC3) recommends all vulnerable systems be patched as soon as practical. Operational testing for newly installed patches may be warranted in some cases

- Patched versions of relevant Citrix systems can be downloaded from the following three links:
  CITRIX ADC – https://www.citrix.com/downloads/citrix-adc/
  CITRIX GATEWAY – https://www.citrix.com/downloads/citrix-gateway/
  CITRIX SD WAN – https://www.citrix.com/downloads/citrix-sd-wan/.

Zoho's ManageEngine service pack release page includes patched builds and can be downloaded here: https://www.manageengine.com/products/desktop-central/service-packs.html

Endnotes

- Citrix. (January 24, 2020). CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance. Citrix.com. Accessed 25 March 2020 at https://support.citrix.com/article/CTX267027
- Clyer, C., Perez, D., Jones, S., and Miller, S. (March 25, 2020). This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits. FireEye.com. Accessed 25 March 2020 at https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
- Lyngass, S. (August 7, 2019). Meet APT41, the Chinese Hackers Moonlighting for Financial Gain. Accessed 25 March 2020 at https://www.cyberscoop.com/apt41-fireeye-china/
- Muncaster, P. (March 25, 2020). APT41 Exploited Cisco, Citrix and Zoho Bugs in Wide-Ranging Campaign. Infosecurity Group. Accessed 25 March 2020 at https://www.infosecurity-magazine.com/news/apt41-exploited-cisco-citrix-and/
- NVD #1. (March 6, 2020). CVE-2020-10189. NIST.gov. Accessed 25 March 2020 at https://nvd.nist.gov/vuln/detail/CVE-2020-10189
- NVD #2. (December 27, 2020). National Vulnerability Database CVE-2019-19781. Accessed 25 March 2020 at https://nvd.nist.gov/vuln/detail/CVE-2019-19781
- SourceIncite. (2020). SRC-2020-0011: ManageEngine Desktop Central FileStorage getChartImage Deserialization of Untrusted Data Remote Code Execution Vulnerability. Srcincite.io. Accessed 25 March 2020 at https://srcincite.io/advisories/src-2020-0011/