Health Sector Cybersecurity Coordination Center (HC3)
Sector Alert
August 13, 2020 TLP: White Report: 202008130700

Citrix Endpoint Management (CEM) AKA XenMobile Server Critical Vulnerabilities

Executive Summary

The XenMobile application is used by many businesses, including those in the HPH sector, and enables businesses to manage employees' mobile devices and mobile applications by controlling device security settings and updates. For example, a healthcare organization might use XenMobile to create an in-house app that allows physicians to view patient information on mobile devices. On August 11, 2020, Citrix released a security bulletin regarding a set of vulnerabilities in certain on-premises instances of Citrix Endpoint Management (CEM), often referred to as XenMobile Server. Some of these vulnerabilities are rated as critical severity and could allow unauthenticated attackers to take over XenMobile Servers following successful exploitation. Citrix recommends updating XenMobile deployments immediately.

Analysis

The critical vulnerabilities affect XenMobile Server 10.12 before RP3, XenMobile Server 10.11 before RP6, XenMobile Server 10.10 before RP6, and XenMobile Server before 10.9 RP5 which allow for arbitrary file read. While Citrix did not provide technical details on the addressed vulnerabilities, the company revealed that it pre-notified CERTs and customers on July 23. According to the security researchers who identified the vulnerability, when following a specially crafted URL, attackers could read arbitrary files outside the web server root directory, including configuration files and encryption keys for sensitive data. No authorization was needed to exploit the vulnerability. One of the two critical flaws discovered, CVE-2020-8209, is a path traversal flaw that results from insufficient input validation. According to Citrix, remediations have already been applied to cloud versions but hybrid rights users need to apply the upgrades to any on-premises instances.

Alert

Critical Vulnerability Exposures (CVEs) associated with this HC3 Alert include:

- CVE-2020-8208 (Critical severity)
- CVE-2020-8209 (Critical severity)
- CVE-2020-8210 (Medium to low severity)
- CVE-2020-8211 (Medium to low severity)
- CVE-2020-8212 (Medium to low severity)

Systems affected by the critical vulnerability include the following:

- XenMobile Server 10.12 before RP3
- XenMobile Server 10.11 before RP6
- XenMobile Server 10.10 before RP6
- XenMobile Server before 10.9 RP5

Patches, Mitigations & Workarounds:

According to Citrix, the latest rolling patches that need to be applied for versions 10.9, 10.10, 10.11, and 10.12 are available immediately. Any versions prior to 10.9.x must be upgraded to a supported version with the latest rolling patch. Citrix recommends upgrading to 10.12 RP3, the latest supported version, immediately. While there are no known exploits at time of writing, malicious actors will likely move quickly to develop an exploit. The latest rolling patches for Citrix Endpoint Management (CEM), also known as XenMobile Server, can be found in the Security Bulletin here: https://support.citrix.com/article/CTX277457

References

Common Vulnerabilities and Exposures (CVEs):
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8209
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8210
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8212

Fermin J. Serna (CISO at Citrix), Citrix provides security update on Citrix Endpoint Management (11 Aug 2020)
https://www.citrix.com/blogs/2020/08/11/citrix-provides-security-update-on-citrix-endpoint-management/
Citrix, Citrix Endpoint Management (CEM) Security Update (11 Aug 2020)
https://support.citrix.com/article/CTX277457
Lindsey O'Donnell (ThreatPost), Citrix Warns of Critical Flaws in XenMobile Server (12 Aug 2020)
https://threatpost.com/citrix-warns-of-critical-flaws-in-xenmobile-server/158293/
Sergui Gatlan, Citrix fixes critical bugs allowing takeover of XenMobile Servers (11 Aug 2020)
https://www.bleepingcomputer.com/news/security/citrix-fixes-critical-bugs-allowing-takeover-of-xenmobile-servers/
Ionet Arghire, Citrix Expects Hackers to Exploit Newly Patched XenMobile Vulnerabilities (11 Aug 2020)
https://www.securityweek.com/citrix-expects-hackers-exploit-newly-patched-xenmobile-vulnerabilities
Positive Technologies, Citrix fixes XenMobile vulnerability found by Positive Technologies (11 Aug 2020)
https://www.ptsecurity.com/ww-en/about/news/citrix-fixes-xenmobile-vulnerability-found-by-positive-technologies/