Security Advisory 2020-040

Critical Vulnerabilities in Citrix XenMobile

August 12, 2020 — v1.0

TLP:WHITE

History:

- *12/08/2020 — v1.0 – Initial publication*

Summary

On 11th of August, Citrix released a blog post [1] and Security Update [2] about critical vulnerabilities affected XenMobile servers products.

No technical details were shared by Citrix, however some sources [3] indicate that by combining some of those vulnerabilities, an unauthenticated attackers could gain admin control on XenMobile Servers if exploitation is successful.

Citrix recommends these upgrades be made immediately. As of this writing, there are no known exploits. However, by analysing security patches, attacker could quickly identify exploits for these vulnerabilities and start scanning for victims exposing XenMobile servers on Internet.

Technical Details

The vulnerabilities were assigned the following CVEs:

- CVE-2020-8208
- CVE-2020-8209
- CVE-2020-8210
- CVE-2020-8211
- CVE-2020-8212

No technical details are available at the time of this writing.

Products Affected

These critical vulnerabilities affect several products:

- XenMobile Server 10.12 before RP2
- XenMobile Server 10.11 before RP4
- XenMobile Server 10.10 before RP6
- XenMobile Server before 10.9 RP5

Other versions of the same products are affected by medium and low vulnerabilities:

- XenMobile Server 10.12 before RP3
- XenMobile Server 10.11 before RP6

Remediations have already been applied to cloud versions of XenMobile server.

Recommendations

Citrix has released Rolling Patches for Citrix Endpoint Management (CEM) [2]:

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

References

[1] https://www.citrix.com/blogs/2020/08/11/citrix-provides-security-update-on-citrix-endpoint-management/

[2] https://support.citrix.com/article/CTX277457

[3] https://www.bleepingcomputer.com/news/security/citrix-fixes-critical-bugs-allowing-takeover-of-xenmobile-servers/