Security Advisory 2020-033

Serious MobileIron Vulnerabilities

November 25, 2020 — v1.1

TLP:WHITE

History:

- *10/07/2020 — v1.0 – Initial publication*
- *25/11/2020 — v1.1 – Update on active exploitation*

Summary

In July 2020, an independent security researcher reported to MobileIron that he had identified vulnerabilities in MobileIron Core that could allow an attacker to execute remote exploits without authentication. MobileIron has issued patches for the affected products [1, 2]. The patches cover three independent vulnerabilities: CVE-2020-15505 (remote code execution), CVE-2020-15506 (authentication bypass), and CVE-2020-15507 (arbitrary file reading).

As of November 2020, proof of concept is available [4], and APT hacking groups are actively utilising CVE-2020-15505 vulnerability to gain access to networks [3].

Technical Details

Description of the issues is available [1]:

CVE-2020-15505 - CVSS 3.0 score 9.8 - CRITICAL:

A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors.

CVE-2020-15507 - CVSS 3.0 score 7.5 - HIGH:

An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors.

CVE-2020-15506 - CVSS 3.0 score 9.8 - CRITICAL

An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors.

Products Affected

- MobileIron Core versions 10.6 and earlier
- MobileIron Sentry versions 9.8 and earlier
- MobileIron Cloud
- Enterprise Connector versions 10.6 and earlier
- Reporting Database (RDB)

Recommendations

Although no CVSS score is available currently, based on the description of the vulnerabilities, CERT-EU strongly advises to apply available patches [2] as soon as possible.

As of November 2020, a proof-of-concept to exploit this vulnerability is publicly available [4]. APT hacking groups are actively utilising CVE-2020-15505 vulnerability to gain access to networks. For example, it was used in the attacks against election support systems in the recent US elections [3].

It is critical to patch CVE-2020-15505 remote code execution (RCE) if not done yet.

References

[1] https://www.mobileiron.com/en/blog/mobileiron-security-updates-available

[2] https://help.mobileiron.com/s/article-detail-page?Id=kA12T000000g065SAA

[3] https://www.bleepingcomputer.com/news/security/hackers-used-vpn-flaws-to-access-us-govt-elections-support-systems/

[4] https://github.com/httpvoid/CVE-Reverse/tree/master/CVE-2020-15505