CERT-EU

Security Advisory 2023-058

Critical Vulnerability in MobileIron Sentry

August 22, 2023 — v1.0

TLP:CLEAR

History:

- *22/08/2023 — v1.0 – Initial publication*

Summary

On July 24, 2023, Ivanti published a security advisory about a vulnerability discovered in Ivanti Sentry, formerly known as MobileIron Sentry [1]. The vulnerability tracked as **CVE-2023-38035** is an API authentication bypass being exploited in the wild. A successful exploitation allows an attacker to change configuration, run system commands, or write files onto systems [3].

While the CVSS score is high (9.8), the software company assessed as a low risk of exploitation for customers who do not expose 8443 to the Internet [2].

Technical Details

Ivanti Sentry acts as a gatekeeper for enterprise ActiveSync servers like Microsoft Exchange Server or backend resources such as Sharepoint servers in MobileIron deployments, and it can also operate as a Kerberos Key Distribution Center Proxy (KKDCP) server [3].

Discovered and reported by researchers at cybersecurity company mnemonic, the critical vulnerability (`CVE-2023-38035`) enables unauthenticated attackers to gain access to sensitive admin portal configuration APIs exposed over port 8443, used by MobileIron Configuration Service (MICS) [3].

Affected Products

This vulnerability affects Ivanti Sentry versions 9.18 and prior.

Recommendations

CERT-EU strongly recommends reviewing Ivanti's security advisory [2] and upgrading affected systems to avoid potential exploitation of this vulnerability.

It is also recommended blocking public access to the admin portal configuration APIs (port 8443), reviewing recent configuration changes and recent file creations on affected devices.

References

[1] https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface?language=en_US

[2] https://www.ivanti.com/blog/cve-2023-38035-vulnerability-affecting-ivanti-sentry

[3] https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-actively-exploited-mobileiron-zero-day-bug/