UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0404

ZERO-DAY VULNERABILITY IN IVANTI SENTRY

DATE ISSUED: 23rd August 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Security researchers have reported a critical authentication bypass vulnerability in Ivanti Sentry (formerly MobileIron Sentry). It could allow an authenticated attacker to gain access to sensitive admin portal configuration Application Programming Interfaces (APIs).

BREAKDOWN

Ivanti is an IT software company that offers asset management solutions. Ivanti Sentry is a gatekeeper for Enterprise ActiveSync servers like Microsoft Exchange or SharePoint servers in MobileIron deployments. A critical Sentry API authentication bypass vulnerability tracked as CVE-2023-38035 has been discovered in the Ivanti Sentry solution. It could allow an authenticated attacker to gain access to sensitive admin portal configuration APIs used by MobileIron Configuration Service (MICS). Successful exploitation could allow attackers to change configuration, run system commands, or write arbitrary files onto systems. Ivanti versions 9.18 or prior are affected by this vulnerability. However, this vulnerability does not affect other Ivanti products or solutions, such as Ivanti EPMM, MobileIron Cloud, or Ivanti Neurons for MDM.

REMEDIATION STEPS

- Upgrade the Ivanti Sentry software to the supported version.
- Admins are advised to avoid exposing MICS to the Internet and restrict access to internal management networks.
- Keep all operating systems, software, and applications updated with the latest security patches to prevent exploitation of known vulnerabilities.

REFERENCES & RESOURCES

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

Ivanti https://www.ivanti.com/blog/cve-2023-38035-vulnerability-affecting-ivanti-sentry