Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Addressed A New Zero-Day Flaw in Ivanti Sentry

Date of Publication	Admiralty Code	TA Number
August 22, 2023	A1	TA2023339

Summary

First Seen: Aug 21, 2023
Affected Platforms: Ivanti Sentry (formerly MobileIron Sentry)
Impact: The zero-day vulnerability (CVE-2023-38035) in Ivanti Sentry (versions 9.18 and earlier) allows unauthenticated access to sensitive APIs via port 8443, posing a risk of configuration manipulation and system compromise. Apply specific RPM scripts and restrict external access for mitigation

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability	Ivanti Sentry	✓	✓	✓

Vulnerability Details

#1

A security vulnerability, CVE-2023-38035, has been discovered in Ivanti Sentry (formerly MobileIron Sentry), affecting versions 9.18 and older versions. Other Ivanti products like Ivanti EPMM, MobileIron Cloud, and Ivanti Neurons for MDM are unaffected. The vulnerability allows unauthorized access to sensitive APIs used for configuring Ivanti Sentry on the administrator portal (port 8443), commonly known as MICS. The CVSS score is 9.8, indicating critical severity, but the risk is lower for users who do not expose port 8443 to the internet.

#2

The vulnerability stems from an Apache HTTPD configuration flaw in the MICS Admin Portal, enabling unauthenticated attackers to bypass authentication controls on the administrative interface. Exploitation could lead to compromising the Sentry system and underlying operating systems, allowing unauthorized execution of system commands. Ivanti has released RPM scripts tailored for each supported version (9.18, 9.17, and 9.16) to address the vulnerability. However, applying the wrong RPM script could result in the vulnerability not being fixed or system instability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-38035	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Apply RPM Scripts Promptly: If you are using Ivanti Sentry version 9.18 or earlier, prioritize the application of the appropriate RPM script provided by Ivanti for your version. Ensure that you select the correct script to fix the vulnerability. Timely installation is crucial to mitigate potential risks.

Secure Access Ports: Limit external access to the administrative interface on port 8443 (MICS). Configure your network or firewall to allow access only from authorized internal management networks, effectively reducing the exposure of the vulnerability to potential attackers.

Regularly Update and Monitor: Keep Ivanti Sentry and associated components up to date by applying security updates and patches. Additionally, implement intrusion detection systems (IDS) or intrusion prevention systems (IPS) to monitor network traffic for signs of unauthorized activities, enhancing early threat detection.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0042 Resource Development	TA0005 Defense Evasion	TA0009 Collection
TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation
T1106 Native API	T1556 Modify Authentication Process	T1543 Create or Modify System Process	T1059 Command and Scripting Interpreter
T1562 Impair Defenses	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits

Patch Details

Action Steps:

- Identify the version of Ivanti Sentry you are using (9.18 or prior).
- Download the corresponding RPM script provided by Ivanti for your version.
- Apply the RPM script as per the provided instructions.
- Verify that the patch has been successfully applied.
- Restrict external access to the System Manager Portal (port 8443) to internal management networks only.

Link:
https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035

References

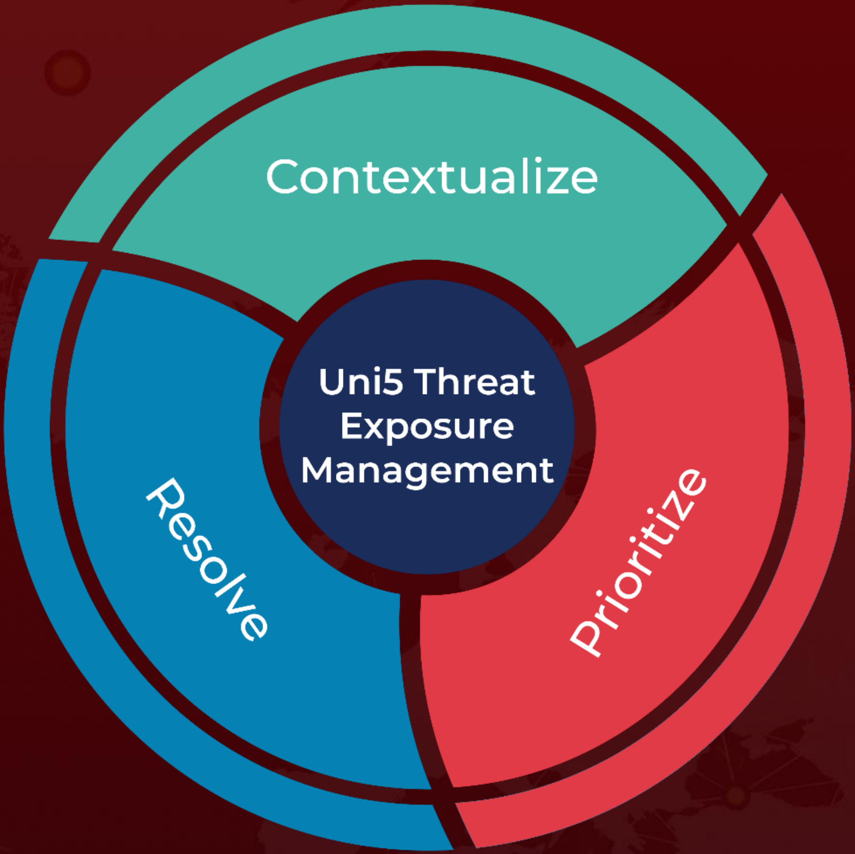
https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 22, 2023 • 7:30 AM

More at www.hivepro.com