Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaw In Ivanti Standalone Sentry Leads To Remote Code Execution

Date of Publication	Admiralty Code	TA Number
March 21, 2024	A1	TA2024112

Summary

Discovered On: March 2024
Affected Products: Ivanti Standalone Sentry
Impact: Ivanti Standalone Sentry has been identified as vulnerable to a critical remote code execution flaw, tracked as CVE-2023-41724. Exploiting this vulnerability, a remote attacker could gain unauthorized access to the target system and execute arbitrary commands.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-41724	Ivanti Standalone Sentry Remote Code Execution Vulnerability	Ivanti Standalone Sentry	❌	❌	✅

Vulnerability Details

#1 A critical vulnerability (CVE-2023-41724) has been identified in Ivanti Standalone Sentry, impacting all supported versions. This vulnerability enables unauthenticated attackers to execute arbitrary commands on affected systems.

#2 CVE-2023-41724 enables a remote attacker to take advantage of insufficient input validation and run arbitrary commands on the victim machine. As a result of this vulnerability, unauthorized users can remotely run OS commands on the compromised system. This vulnerability has the potential to completely compromise the susceptible system if it is successfully exploited.

#3 As of the disclosure, there have been no reported instances of threat actors exploiting this vulnerability. However, it's important to note that threat actors could potentially exploit the vulnerability over the Internet if they possess a valid TLS client certificate enrolled through EPMM.

#4 Ivanti has addressed CVE-2023-41724 in the latest version of Ivanti Standalone Sentry. Threat actors have been capitalizing on multiple Ivanti vulnerabilities since the beginning of the year, deploying different strains of tailored malware, underscoring the need of immediate patching.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-41724	Ivanti Standalone Sentry: Versions 9.17.0, 9.18.0, and 9.19.0 and older	cpe:2.3:a:ivanti:standalonesentry:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Patch: Install the security patch provided by Ivanti to address the CVE-2023-41724 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	

Patch Details

Ivanti has released patches to address the CVE-2023-41724 in the latest versions 9.17.1, 9.18.1 and 9.19.1

Link:
https://help.ivanti.com/mi/help/en_us/SNTRY/9.x/rn/RelnotesStandaloneSentry/Software_download_%20for_Standalone%20Sentry.htm

References

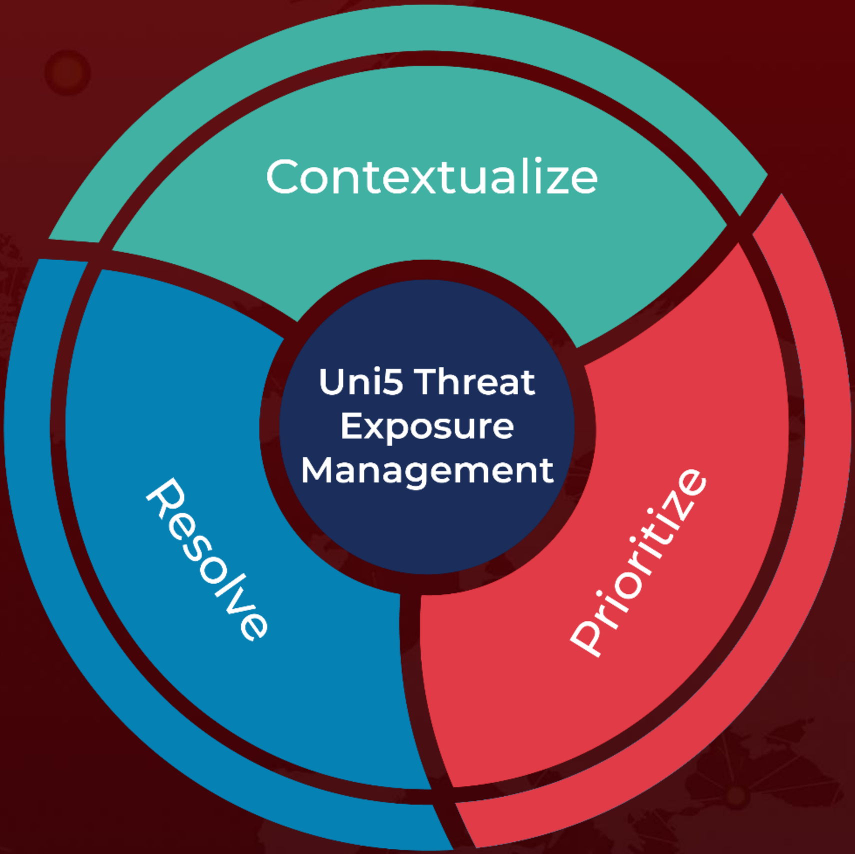
https://forums.ivanti.com/s/article/KB-CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry

https://www.hivepro.com/threat-advisory/ivanti-gateways-under-attack-by-cybercriminals-patch-now/

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

March 21, 2024 • 6:20 AM

More at www.hivepro.com