

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Ivanti Addresses Critical Vulnerability in Endpoint Manager

Date of Publication

January 5, 2024

Admiralty Code

A1

TA Number

TA2024007




Summary

First Seen: Jan 4, 2024

Affected Platform: Ivanti Endpoint Manager

Impact: Ivanti addressed a critical vulnerability (CVE-2023-39336) in its Endpoint Management software, ensuring secure usage for its 40,000 worldwide customers. The flaw, resolved in version 2022 Service Update 5, posed a risk of pre-authenticated sql injection and possibly Remote Code Injection in case of core server.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-39336	Ivanti Endpoint Manager SQL injection Vulnerability	Ivanti Endpoint Manager			

Vulnerability Details

#1

Ivanti, a prominent provider of IT asset and system management solutions, has addressed a critical vulnerability (CVE-2023-39336) in its Endpoint Management software (EPM). The flaw posed a significant risk, potentially allowing unauthenticated attackers to take control of devices or the core server.

#2

This vulnerability, affecting all supported EPM versions, was promptly resolved in version 2022 Service Update 5, ensuring secure software usage. The flaw, exploitable through an unspecified SQL injection method, could grant attackers access to the internal network, execute arbitrary SQL queries, and retrieve sensitive data.

#3

Ivanti temporarily restricted public access to details, demonstrating a commitment to security. Despite no evidence of customer exploitation, the incident raises concerns in the context of previous zero-day vulnerabilities exploited by state-affiliated hackers in Ivanti's products for cyberattacks, including in [Ivanti Endpoint Manager Mobile \(EPMM\)](#) and [Ivanti Sentry](#).

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-39336	Ivanti Endpoint Manager: Before 2022 SU5	cpe:2.3:a:ivanti:ivanti_endpoint_manager:*:*:*:*:*:*	CWE-89

Recommendations



Apply Security Updates: Immediately apply the security updates provided by Ivanti. Ensure that the EPM software is updated to version 2022 Service Update 5 or later to address CVE-2023-39336. Regularly check for and apply software updates and patches to address any newly discovered vulnerabilities.



Deploy Anomaly Detection and Monitoring: Implement network monitoring tools with anomaly detection capabilities to identify unusual or suspicious patterns of network activity. This can include unexpected increases in data traffic, unusual access patterns, or deviations from normal behavior.



Network Segmentation: Employ network segmentation to isolate email security appliances from critical internal networks. This can help contain the impact of a potential breach and prevent lateral movement within the network.



Database Security: Implement secure coding practices to prevent SQL injection vulnerabilities. Regularly audit and secure database configurations to minimize the risk of unauthorized access to sensitive data.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities
<u>T1203</u> Exploitation for Client Execution	<u>T1588.005</u> Exploits		

Patch Details

Upgrade Ivanti Endpoint Manager (EPM) software to version 2022 Service Update 5 or later

Link:

<https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336>

References

<https://thehackernews.com/2024/01/alert-ivanti-releases-patch-for.html>

<https://www.hivepro.com/threat-advisory/ivanti-addressed-second-zero-day-flaw-exploited-by-attackers/>

<https://www.hivepro.com/threat-advisory/ivanti-addressed-a-new-zero-day-flaw-in-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

January 5, 2024 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro[®]



More at www.hivepro.com