

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Active Exploitation of Critical Flaws in Ivanti EPM

Date of Publication

September 18, 2024

Last updated date

October 4, 2024

Admiralty Code

A1

TA Number

TA2024360







Summary

First Seen: May 2024

Affected Product: Ivanti Endpoint Manager

Impact: Ivanti has patched two critical vulnerabilities, CVE-2024-29824 and CVE-2024-29847, in its Endpoint Manager (EPM). These flaws allow unauthenticated attackers to execute arbitrary code, leading to full system compromise. CVE-2024-29847 involves insecure deserialization, while CVE-2024-29824 is an SQL injection vulnerability. Both are actively exploited, and proof-of-concept (PoC) exploit code is publicly available, making immediate patching essential.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-29847	Ivanti Endpoint Manager Deserialization of Untrusted Data Vulnerability	Ivanti Endpoint Manager (EPM)			
CVE-2024-29824	Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability	Ivanti Endpoint Manager (EPM)			

Vulnerability Details

#1

Ivanti has patched multiple critical vulnerabilities in its Endpoint Manager (EPM), specifically CVE-2024-29824 and CVE-2024-29847. Both are severe vulnerabilities affecting EPM appliances, particularly those running versions prior to 2022 SU5.

#2

These vulnerabilities allow unauthenticated attackers within the same network to execute arbitrary code on the affected systems, potentially allowing them to take full control, steal data, or launch additional attacks. The critical nature of these vulnerabilities has made them a prime target for exploitation by cybercriminals.

#3

CVE-2024-29847 involves an insecure deserialization flaw in the AgentPortal.exe component. By sending a maliciously crafted Hashtable to a vulnerable system, attackers can exploit this flaw during deserialization to execute arbitrary operations like file reading/writing or launching web shells. This can lead to full system compromise.

#4

CVE-2024-29824 is an unauthenticated SQL injection vulnerability found in the PatchBiz.dll file, affecting EPM versions 2022 SU5 and earlier. Attackers can manipulate SQL queries through improper input handling, leading to remote code execution using the xp_cmdshell command.

#5

Both vulnerabilities are already being actively exploited in the wild, and the availability of proof-of-concept (PoC) exploit code significantly increases the urgency for administrators to apply the 2022 SU6 or September 2024 updates, as no workarounds are available

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-29847	Ivanti Endpoint Manager 2022 SU5 and prior Ivanti Endpoint Manager 2024	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:* *	CWE-502
CVE-2024-29824	Ivanti Endpoint Manager 2022 SU5 and prior versions	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:* *	CWE-89

Recommendations



Apply Patches and Updates: Immediately update Ivanti Endpoint Manager to version 2022 SU6 or the September 2024 release, as these patches address this vulnerability. This is the only effective mitigation, with no available workarounds.



Monitor Network Traffic: Regularly review logs and monitor network traffic for any unexpected connections to the **AgentPortal** service, which could indicate attempts to exploit this vulnerability. Use security tools like intrusion detection systems (IDS) and endpoint protection to detect suspicious behavior.



Disable xp_cmdshell: For CVE-2024-29824, disable the xp_cmdshell feature in SQL Server if it is not required. This feature is often exploited for remote code execution in SQL injection attacks. Disabling it limits the scope of SQL injection attacks.



Strengthen File Execution Policies: Restrict execution of potentially dangerous file types, such as .hta and .exe, especially from untrusted sources. This can help prevent malicious scripts from running even if they bypass detection methods.



Backup Systems: Before applying the patches, ensure that critical systems and data are backed up to avoid potential data loss or downtime during the update process. This precaution will help maintain operational continuity in case of unforeseen issues



Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>T1059</u> Command and Scripting Interpreter
<u>T1190</u> Exploit Public-Facing Application	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1203</u> Exploitation for Client Execution			



Patch Details

Upgrade Ivanti Endpoint Manager to latest versions 2022 SU6 and EPM 2024 or later.

Links:

<https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022>

<https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024>

References

<https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022>

<https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024>

<https://www.horizon3.ai/attack-research/attack-blogs/cve-2024-29824-deep-dive-ivanti-epm-sql-injection-remote-code-execution-vulnerability/>

<https://exploitpoccom.wordpress.com/2024/06/13/cve-2024-29824-exploit-poc-ivanti-epm-sql-injection-remote-code-execution-vulnerability/>

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

September 18, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com