Ivanti Endpoint Manager Vulnerabilities Allow Remote Code Execution

TL;DR

Ivanti released an update for Endpoint Manager (EPM) after researchers discovered a stored XSS flaw and three high-severity weaknesses that can lead to remote code execution or arbitrary file writes.

All issues are fixed in EPM 2024 SU4 SR1. No exploitation has been confirmed, but hundreds of EPM servers remain exposed online.

Overview

Ivanti issued a security update to fix four vulnerabilities affecting Endpoint Manager versions 2024 SU4 and earlier. The most severe issue, CVE-2025-10573 (CVSS 9.6), lets an unauthenticated attacker inject malicious JavaScript into the EPM dashboard by registering fake endpoints. When an administrator later views the poisoned dashboard, the attacker can take over that session. The flaw requires user interaction, but the impact is high because the attacker ends up with the administrator's privileges.

Ivanti also addressed three additional vulnerabilities, CVE-2025-13659, CVE-2025-13661, and CVE-2025-13662. Each one can lead to code execution under the right conditions. While these issues require specific user actions such as connecting to an untrusted server or importing an untrusted configuration file, history shows that EPM vulnerabilities draw interest from attackers once technical details are public.

Affected Products

- Ivanti Endpoint Manager 2024 SU4 and earlier
- Fixed in EPM 2024 SU4 SR1 (available through the Ivanti License System)

Shadowserver data shows hundreds of Internet-facing EPM instances, despite Ivanti's guidance that the product should not be online at all.

Vulnerability Breakdown

- CVE-2025-10573 (CVSS 9.6) - Stored XSS that lets an unauthenticated attacker inject JavaScript into the admin dashboard by registering fake endpoints. When an admin loads the interface, that script runs inside their session, giving the attacker control of the account.
- CVE-2025-13659 (CVSS 8.8) - Improper control of code resources allows an unauthenticated attacker to write arbitrary files to the server. With the right conditions, this can be used to reach remote code execution. User interaction is required.

- CVE-2025-13661 (CVSS 7.1) - A path-traversal bug that lets an authenticated user write files outside intended directories. Requires user interaction.
- CVE-2025-13662 (CVSS 7.8) - Improper signature verification in patch management, allowing malicious files to execute when an administrator imports untrusted configuration data.

Most exposed systems are in the U.S., Germany, and Japan. Although Ivanti says it has no evidence of exploitation so far, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** - Install EPM 2024 SU4 SR1 as soon as possible.
- Confirm EPM servers are not exposed to the public Internet.
- Restrict connections to trusted core servers only.
- Allow only trusted configuration files to be imported into EPM.
- Monitor admin sessions for unusual behavior, especially after dashboard activity.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may attempt to add fake endpoints to gain a foothold inside the system.
- Exploit Public-Facing Application [T1190] – If the EPM interface is exposed online, an unauthenticated attacker can exploit the XSS flaw.

Execution

- User Execution [T1204] – The attacker depends on an admin loading a poisoned dashboard or importing an untrusted file.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker may gain administrator-level access once malicious JavaScript runs.

Impact

- Data Manipulation [T1565] – Arbitrary file-write vulnerabilities could let the attacker alter system files or deploy malicious payloads.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This Ivanti EPM vulnerability affects any organization using Endpoint Manager for device administration and patch management.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Security Advisory EPM December 2025 for EPM 2024

CVE-2025-10573: Ivanti EPM Unauthenticated Stored Cross-Site Scripting (Fixed)