

POSTING DATE: 2025/12/17

[VULNERABILITY ALERT] Ivanti's EPM Has 2 Critical Security Vulnerabilities (CVE-2025-10573) (CVE-2025-13659)

- Subject: [VULNERABILITY ALERT] Ivanti's EPM Has 2 Critical Security Vulnerabilities (CVE-2025-10573) (CVE-2025-13659)
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202512-00000004
 - Ivanti's Endpoint Manager (EPM) is a system specialized for device management, providing management and protection for Windows, macOS, and Linux devices.
 - [CVE-2025-10573, CVSS: 9.6] This is a Stored Cross-Site Scripting (XSS) vulnerability, allowing a remote unauthenticated attacker to execute arbitrary JavaScript code in an administrator session.
 - [CVE-2025-13659, CVSS: 8.8] This is an Arbitrary File Write vulnerability, due to improper control over dynamically managed code resources, allowing a remote unauthenticated attacker to write arbitrary files on the server, which may lead to Remote Code Execution.
- Affected Platforms:
 - EPM versions up to and including 2024 SU4
- Recommended Actions:
 - Please update to the following version: EPM 2024 SU4 SR1 version

Computer and Communication Center
Network Systems Division, Respectfully

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251217_02



Last update: **2025/12/17 11:26**