مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ivanti Endpoint Manager (EPM) December 2025 Update

Tracking #:432318114

Date:10-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti has released a security update for Ivanti Endpoint Manager (EPM) addressing four vulnerabilities—one critical and three high-severity—that impact the EPM core and remote consoles.

TECHNICAL DETAILS:

Ivanti has released a security update for Ivanti Endpoint Manager (EPM) addressing four vulnerabilities—one critical and three high-severity—that impact the EPM core and remote consoles. These vulnerabilities include stored cross-site scripting, arbitrary file write, path traversal, and improper cryptographic validation issues that could enable remote code execution (RCE), unauthorized file manipulation, and administrative compromise.
No exploitation has been observed in the wild at the time of disclosure. Customers are strongly advised to upgrade to EPM 2024 SU4 SR1 immediately and apply recommended hardening practices to minimize exposure.

Vulnerability Details:

1. CVE-2025-10573 – Stored Cross-Site Scripting (XSS)
   - Severity: Critical (CVSS 9.6)
   - CWE: 79 – Improper Neutralization of Input During Web Page Generation
   - Description:
     A stored XSS flaw in EPM prior to 2024 SU4 SR1 allows a remote unauthenticated attacker to inject malicious JavaScript that executes in the context of an administrator session. Exploitation requires user interaction.

2. CVE-2025-13659 – Arbitrary File Write Leading to Potential RCE
   - Severity: High (CVSS 8.8)
   - Description:
     Improper validation of dynamic resources enables a remote unauthenticated attacker to write arbitrary files to the server, potentially enabling remote code execution. User interaction required.

3. CVE-2025-13661 – Authenticated Path Traversal File Write
   - Severity: High (CVSS 7.1)
   - Description:
     A directory traversal flaw allows a remote authenticated attacker to write files outside permitted directories. User interaction required.

4. CVE-2025-13662 – Improper Cryptographic Signature Verification
   - Severity: High (CVSS 7.8)
   - Description:
     The patch management component does not properly validate cryptographic signatures, allowing a remote unauthenticated attacker to execute arbitrary code if a user imports a malicious file.

Affected Versions:

Product	Affected Versions	Fixed Version
Ivanti Endpoint Manager	2024 SU4 and earlier	2024 SU4 SR1

RECOMMENDATIONS:

1. **Apply the Security Update**
   - Upgrade all EPM core and remote consoles to EPM 2024 SU4 SR1.
   - Ensure no outdated remote consoles remain connected.
2. **Validate Server Exposure**
   - Ensure EPM is not exposed to the public internet, mitigating CVE-2025-10573.
   - Restrict EPM access to internal networks only.
3. **Restrict Connections to Trusted Servers**
   - For CVE-2025-13659, ensure that endpoints only connect to trusted EPM core servers.
   - Validate server certificates and configurations.
4. **Tighten Import Controls**
   - Only import trusted configuration or patch files, reducing risk of CVE-2025-13661 & CVE-2025-13662.
   - Implement file validation and content-signature checks where applicable.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024?language=en_US&_gl=1*ly49vh*_gcl_au*NTk3NTg0Mzg2LjE3NjUzMzk5MjQ.