NCSC
National Cyber Security Centre

2411140370-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Critical Vulnerabilities in Ivanti EPM
EPM November 2024 for EPM 2024 and EPM 2022 SU6
UPDATE 1.1

Monday 18th November, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	12th September 2024	CSIRT-IE	Initial advisory responding to Ivanti advisory
1.1	12th November 2024	CSIRT-IE	Updates for Ivanti Endpoint Manager which addresses high and critical severity vulnerabilities.

Description

CVE ID: CVE-2024-50330

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0**[1] **Score** 9.8 (Critical)
- **EPSS**[2]**:** 0.316490000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-50330)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote unauthenticated attacker to achieve remote code execution.
- **Common Weakness Enumeration (CWE)**[3]**:** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE ID: CVE-2024-50329

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 8.8 (High)
- **EPSS:** 0.316490000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-50329)
- **Summary:** Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.
- **Common Weakness Enumeration (CWE):** CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE IDs: CVE-2024-34787, CVE-2024-50322

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 7.8 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here:
  https://api.first.org/data/v1/epss?cve=CVE-2024-34787
  https://api.first.org/data/v1/epss?cve=CVE-2024-50322
- **Summary:** Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a local unauthenticated attacker to achieve code execution. User interaction is required.
- **Common Weakness Enumeration (CWE):** CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

[1] https://www.first.org/cvss/v3.0/specification-document

[2] https://www.first.org/epss/articles/prob_percentile_bins

[3] https://cwe.mitre.org/

CVE ID: CVE-2024-32839, CVE-2024-32841, CVE-2024-32844

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 7.2 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32839 https://api.first.org/data/v1/epss?cve=CVE-2024-32841 https://api.first.org/data/v1/epss?cve=CVE-2024-32844)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE IDs: CVE-2024-32847, CVE-2024-34780, CVE-2024-37376

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score** 7.2 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32847 https://api.first.org/data/v1/epss?cve=CVE-2024-34780 https://api.first.org/data/v1/epss?cve=CVE-2024-37376)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE ID: CVE-2024-34781, CVE-2024-34782, CVE-2024-34784

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 7.2 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-34781 https://api.first.org/data/v1/epss?cve=CVE-2024-34782 https://api.first.org/data/v1/epss?cve=CVE-2024-34784)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE ID: CVE-2024-50323

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 7.8 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-50323)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a local unauthenticated attacker to achieve code execution. User interaction is required.
- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE ID: CVE-2024-50324

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM
- **CVSS3.0 Score:** 7.2 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-50324)
- **Summary:** Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE IDs: CVE-2024-50326, CVE-2024-50327, CVE-2024-50328

- **Published:** 2024-11-12T15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 7.2 (High)
- **EPSS:** 0.095720000 (For up to date EPSS score, see here:
  https://api.first.org/data/v1/epss?cve=CVE-2024-50326
  https://api.first.org/data/v1/epss?cve=CVE-2024-50327
  https://api.first.org/data/v1/epss?cve=CVE-2024-50328)
- **Summary:** SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Products Affected

Ivanti Endpoint Manager (EPM)

- 2024 September security update and prior
- 2022 SU6 September security update and prior

Impact

Present in CISA Known Exploited Vulnerability(KEV)[4] catalog: NO
Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Ivanti.

Additional recommendations and mitigations can be found in the respective link below:

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022?language=en_US

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber Security Centre