National Cyber Security Centre

2409120152-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Critical Vulnerabilities in Ivanti EPM

Friday 13th September, 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.

Description

CVE ID: CVE-2024-29847

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 10.0
- **EPSS**[1]**:** 0.316490000
  (For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-29847
- **Summary:** Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.
- **Common Weakness Enumeration (CWE):** CWE-502 Deserialization of untrusted data

CVE ID: CVE-2024-37397

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0**[2] **Score** 8.2
- **EPSS**[3]**:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-37397)
- **Summary:** An External XML Entity (XXE) vulnerability in the provisioning web service of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to leak API secrets.
- **Common Weakness Enumeration (CWE):** CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVE ID: CVE-2024-32840

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32840)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.

[1] https://www.first.org/epss/articles/prob_percentile_bins
[2] https://www.first.org/cvss/v3.0/specification-document
[3] https://www.first.org/epss/articles/prob_percentile_bins

- **Common Weakness Enumeration (CWE):** CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVE ID: CVE-2024-32842

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32842)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-32843

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32843)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-32845

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32845)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-32846

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32846)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-32848

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-32848)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-34779

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-34779)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-34783

- **Published:** 2024-09-12T02:15:00

- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-34783)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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-2024-34785

- **Published:** 2024-09-12T02:15:00
- **Vendor:** Ivanti
- **Product:** EPM;
- **CVSS3.0 Score:** 9.1
- **EPSS:** 0.095720000
  (For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-34785)
- **Summary:** An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September 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 EPM before 2022 SU6 or the 2024 September update.

Impact

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

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

Recommendations

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

Additional recommendations and mitigation's can be found in the respective link below:

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

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