Security Advisory 2024-094

Critical Vulnerabilities in Ivanti EPM

2024-09-11 — v1.0

TLP:CLEAR

History:

- *11/09/2024 — v1.0 – Initial publication*

Summary

On September 10, 2024, Ivanti addressed several critical and high security vulnerabilities its Endpoint Manager (EPM) product [1].

It is recommended updating as soon as possible.

Technical Details

The most severe vulnerability, **CVE-2024-29847**, with a CVSS score of 10, is due to improper input validation which could lead to deserialisation of untrusted data in the agent portal of Ivanti EPM. It could allow a remote unauthenticated attacker to achieve remote code execution.

The vulnerabilities **CVE-2024-32840**, **CVE-2024-32842**, **CVE-2024-32843**, **CVE-2024-32845**, **CVE-2024-32846**, **CVE-2024-32848** and **CVE-2024-34779**, with a CVSS score of 9.1, are SQL injection flaws in Ivanti EPM. They could allow an authenticated remote attacker with admin privileges to achieve remote code execution on the server.

Affected Products

The following product versions are affected [1]:

- Ivanti Endpoint Manager (EPM) 2022 SU5 and earlier.
- Ivanti Endpoint Manager (EPM) 2024.

Recommendations

CERT-EU strongly recommends updating affected devices as soon as possible.

References

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