Security Advisory 2024-041

Multiple Vulnerabilities in Ivanti Avalanche MDM

April 17, 2024 — v1.0

TLP:CLEAR

History:
• 17/04/2024 — v1.0 – Initial publication

Summary

On April 16, 2024, Ivanti disclosed several vulnerabilities in its Avalanche MDM solution, including two critical heap overflow issues allowing unauthenticated remote command execution [1]. It is recommended updating as soon as possible.

Technical Details

The two critical security flaws, tracked as CVE-2024-24996 and CVE-2024-29204, with CVSS score of 9.8, were found in Avalanche’sWLInfoRailService and WLашavencheService components [1]. They are both caused by heap-based buffer overflow weaknesses, which can let unauthenticated remote attackers execute arbitrary commands on vulnerable systems in low-complexity attacks that do not require user interaction [1].

The 25 other vulnerabilities are ranging from medium to high severity, and can lead to denial of service conditions, unauthorised command execution as SYSTEM, and sensitive information disclosure [2].

Affected Products

Avalanche MDM versions before version 6.4.3.

Recommendations

CERT-EU recommends updating to the fixed version as soon as possible [2].
References
