CERT-EU

Security Advisory 2023-099

Critical Vulnerabilities in Ivanti Avalanche

December 21, 2023 — v1.0

TLP:CLEAR

History:

- *21/12/2023 — v1.0 – Initial publication*

Summary

On December 20, 2023, Ivanti has released security updates to fix 13 critical security vulnerabilities in the company's Avalanche enterprise mobile device management (MDM) solution. These vulnerabilities, if exploited, could lead to Remote Code Execution or Denial of Service [1,2]. The updates also cover 8 medium- and high-severity bugs that attackers could exploit in denial of service, remote code execution, and server-side request forgery (SSRF) attacks.

It is strongly recommended updating as soon as possible.

Technical Details

The 13 critical security vulnerabilities, all with a CVSS score of 9.8, could be exploited by remote attackers sending specially crafted data packets to the Mobile Device Server to cause memory corruption (buffer overflow) which could result in a Denial of Service (DoS) or code execution. The vulnerabilities include: `CVE-2023-41727`, `CVE-2023-46216`, `CVE-2023-46217`, `CVE-2023-46220`, `CVE-2023-46221`, `CVE-2023-46222`, `CVE-2023-46223`, `CVE-2023-46224`, `CVE-2023-46225`, `CVE-2023-46257`, `CVE-2023-46258`, `CVE-2023-46259`, `CVE-2023-46260`, and `CVE-2023-46261`.

- The vulnerability `CVE-2023-46260`, with a CVSS score of 7.5, is caused by a Null Pointer Dereference that, if exploited, could lead to a Denial of Service condition.
- The vulnerability `CVE-2023-46262`, with a CVSS score of 7.5, could be exploited by an unauthenticated attacker sending a specifically crafted web request causing a Server-Side Request Forgery (SSRF) in Ivanti Avalanche Remote Control server.
- The vulnerability `CVE-2023-46266`, with a CVSS score of 7.3, could be exploited by an attacker sending a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack.
- The vulnerabilities `CVE-2023-46263` and `CVE-2023-46264`, with a CVSS score of 7.2, could allow an attacker to upload of files with dangerous type in Avalanche and to achieve a remove code execution.

- The vulnerabilities `CVE-2023-46803` and `CVE-2023-46804`, with a CVSS score of 7.5, could be exploited by an attacker sending specially crafted data packets to the Mobile Device Server to cause a Denial of Service (DoS).
- The vulnerability `CVE-2023-46265`, with a CVSS score of 6.5, could be exploited by an unauthenticated attacker to leak data or perform a Server-Side Request Forgery (SSRF) on the Smart Device Server.

Affected Products

These vulnerabilities affect at least Ivanti Avalanche versions 6.4.1 and 6.4.2. According to Ivanti, these vulnerabilities highly likely affect all Avalanche versions 6.X [2].

Recommendations

It is strongly recommended updating as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/ivanti-releases-patches-for-13-critical-avalanche-rce-flaws/

[2] https://forums.ivanti.com/s/article/Avalanche-6-4-2-Security-Hardening-and-CVEs-addressed?language=en_US