



CVE-2023-32560

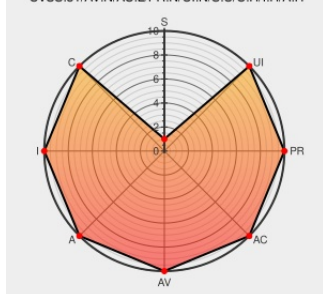
Published on: Not Yet Published

Last Modified on: 09/18/2023 04:15:00 PM UTC

CVE-2023-32560

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Avalanche](#) from [Ivanti](#) contain the following vulnerability:

An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in service disruption or arbitrary code execution. Thanks to a Researcher at Tenable for finding and reporting. Fixed in version 6.4.1.

CVE-2023-32560 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [h1](#) **Ivanti - Avalanche** version **not down converted**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Ivanti Avalance Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/174459/Ivanti-Avalance-Remote-Code-Execution.html
Ivanti Avalanche MDM Buffer Overflow ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/174698/Ivanti-Avalanche-MDM-Buffer-Overflow.html
Ivanti Community	forums.ivanti.com text/html	MISC forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Avalanche	All	All	All	All
cpe:2.3:a:ivanti:avalanche:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/cybersecurity_news	Critical Security Flaws Affect Ivanti Avalanche, Threatening 30,000 Organizations	2023-08-17 13:49:27
 /r/msp	APG Threat Digest	2023-08-21 16:06:22

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)