



# Ivanti Sentry Authentication Bypass Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-38035
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-21 17:15:00 UTC
<b>Updated</b>	2023-09-13 18:15:00 UTC
<b>Description</b>	A security vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry versions 9.18.0 and below, which may allow an attacker to bypass authentication and gain access to the system.

## Risk And Classification

**EPSS:** 0.944190000 probability, percentile 0.999790000 (date 2026-04-21)

**CISA KEV:** Listed on 2023-08-22; due 2023-09-12; ransomware use Known

**Problem Types:** CWE-863

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Ivanti
<b>Product</b>	Sentry
<b>Name</b>	Ivanti Sentry Authentication Bypass Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface?language=en_US</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-38035">https://nvd.nist.gov/vuln/detail/CVE-2023-38035</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	MobileIron Sentry	All	All	All	All

## References

Reference	Source	Link	Tags
Ivanti Community	MISC	<a href="https://forums.ivanti.com">forums.ivanti.com</a>	
Ivanti Sentry Authentication Bypass / Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

<a href="#">NVD vulnerability detail</a>	<a href="#">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	<a href="#">Canonical, analysis</a>
<a href="#">CISA Known Exploited Vulnerabilities catalog</a>	<a href="#">CISA</a>	<a href="https://www.cisa.gov">www.cisa.gov</a>	<a href="#">kev</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[730875](#) Ivanti Sentry Authentication Bypass Vulnerability (Zero Day)

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)