



CVE-2026-8111

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

Summary

CVE	CVE-2026-8111
State	PUBLISHED
Assigner	ivanti
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 15:16:18 UTC
Updated	2026-05-12 19:17:48 UTC
Description	SQL injection in the web console of Ivanti Endpoint Manager before version 2024 SU6 allows a remote authenticated attack

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from 3c1d8aa1-5a33-4ea4-8992-aadd6440af75

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-89 | CWE-89 CWE-89 Improper neutralization of special elements used in an SQL command ('SQL injection')

Version	Source	Type	Score	Severity	Vector
3.1	3c1d8aa1-5a33-4ea4-8992-aadd6440af75	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Endpoint Manager	2024	-	All	All
Application	Ivanti	Endpoint Manager	2024	su1	All	All
Application	Ivanti	Endpoint Manager	2024	su2	All	All
Application	Ivanti	Endpoint Manager	2024	su3	All	All
Application	Ivanti	Endpoint Manager	2024	su3_security_release_1	All	All
Application	Ivanti	Endpoint Manager	2024	su4	All	All
Application	Ivanti	Endpoint Manager	2024	su4_security_release_1	All	All
Application	Ivanti	Endpoint Manager	2024	su5	All	All
Application	Ivanti	Endpoint Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ivanti	Endpoint Manager	unaffected 2024 SU6	Not specified

References

Reference	Source	Link
hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-May-2026	3c1d8aa1-5a33-4ea4-8992-aadd6440af75	hub.ivanti.c
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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

CVE.report and Source URL Uptime Status status.cve.report