



CVE-2025-48700

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

Summary

CVE	CVE-2025-48700
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-23 15:15:27 UTC
Updated	2026-04-21 12:48:23 UTC
Description	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0 and 10.0 and 10.1. A Cross-Site Scripting (XSS) vul

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from ADP

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

EPSS: 0.345110000 probability, percentile 0.970100000 (date 2026-04-21)

CISA KEV: Listed on 2026-04-20; due 2026-04-23; ransomware use Unknown

Problem Types: CWE-79 | n/a | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

CISA Known Exploited Vulnerability

Vendor	Synacor
Product	Zimbra Collaboration Suite (ZCS)
Name	Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories ; https://nvd.nist.gov/vuln/detail/CVE-2025-48700

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synacor	Zimbra Collaboration Suite	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
wiki.zimbra.com/wiki/Zimbra_Responsible_Disclosure_Policy	cve@mitre.org	wiki.zimbra.com	Product
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Governmen
wiki.zimbra.com/wiki/Security_Center	cve@mitre.org	wiki.zimbra.com	Release Notes
wiki.zimbra.com/wiki/Zimbra_Security_Advisories	cve@mitre.org	wiki.zimbra.com	Vendor Advisor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
--------	------	-------

ADP

2026-04-20T00:00:00.000Z

CVE-2025-48700 added to CISA KEV

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](#)