



# Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability

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

## Summary

<b>CVE</b>	CVE-2023-37580
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-31 16:15:00 UTC
<b>Updated</b>	2023-11-17 15:15:00 UTC
<b>Description</b>	Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41 allows XSS in the Zimbra Classic Web Client.

## Risk And Classification

**EPSS:** 0.939180000 probability, percentile 0.998790000 (date 2026-04-22)

**CISA KEV:** Listed on 2023-07-27; due 2023-08-17; ransomware use Unknown

**Problem Types:** CWE-79

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Synacor
<b>Product</b>	Zimbra Collaboration Suite (ZCS)
<b>Name</b>	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) 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://wiki.zimbra.com/wiki/Security_Center">https://wiki.zimbra.com/wiki/Security_Center</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-37580">https://nvd.nist.gov/vuln/detail/CVE-2023-37580</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	All	All	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p11	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p26	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p3	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p30	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p31	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p32	All	All

Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p33	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p34	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p35	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p37	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p38	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p40	All	All
Application	<a href="#">Zimbra</a>	<a href="#">Zimbra</a>	8.8.15	p5	All	All

## References

Reference	Source	Link	Tags
Zimbra Responsible Disclosure Policy - Zimbra :: Tech Center	MISC	<a href="http://wiki.zimbra.com">wiki.zimbra.com</a>	
<a href="http://wiki.zimbra.com/wiki/Security_Center">wiki.zimbra.com/wiki/Security_Center</a>	MISC	<a href="http://wiki.zimbra.com">wiki.zimbra.com</a>	
oss-security - CVE-2023-37580 (and others): XSS vulnerabilities in Zimbra Collaboration Suite		<a href="http://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

378721 Zimbra Cross-Site Scripting (XSS) Vulnerability (CVE-2023-37580)

© [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](http://cve.report/api)

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