



# CVE-2023-39115

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

## Summary

<b>CVE</b>	CVE-2023-39115
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-16 15:15:00 UTC
<b>Updated</b>	2023-08-22 18:14:00 UTC
<b>Description</b>	install/ai-z-uploader/upload in Campcodes Online Matrimonial Website System Script 3.3 allows XSS via a crafted SVG doc

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Campcodes	Complete Online Matrimonial Website System Script	3.3	All	All	All

## References

Reference	Source
GitHub - Raj789-sec/CVE-2023-39115: Campcodes Online Matrimonial Website System 3.3 Cross Site Scripting	MISC
Campcodes Online Matrimonial Website System 3.3 Cross Site Scripting ≈ Packet Storm	MISC
Complete Online Matrimonial Website System Script In PHP MySQL   CampCodes	MISC
Campcodes Online Matrimonial Website System v3.3 - Code Execution via malicious SVG file upload - PHP webapps Exploit	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)**