CVE-2023-39600

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-39600
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-25 20:15:00 UTC
Updated	2023-11-07 04:17:00 UTC
Description	IceWarp 11.4.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the color parameter.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icewarp	Icewarp	11.4.6.0	All	All	All

References

Reference	Source	Li
Cross Site Scripting (Reflected-XSS) in IceWarp Server (CVE-2023–39600) | by Sushmitha Katikitala | Aug, 2023 | Medium		me
icewrap.com | Venture	MISC	ice
Cross Site Scripting (Reflected-XSS) in IceWarp Server (CVE-2023–39600) | by Sushmitha Katikitala | Aug, 2023 | Medium	MISC	me
IceWarp® - Business Email Server & Collaboration Hub	MISC	ice
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730908 IceWarp Server Cross-Site Scripting (XSS) Vulnerability

© 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 registred 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**