



CVE-2022-39285

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

Summary

CVE	CVE-2022-39285
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-07 21:15:00 UTC
Updated	2023-03-27 18:15:00 UTC
Description	ZoneMinder is a free, open source Closed-circuit television software application The file parameter is vulnerable to a cross

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoneminder	Zoneminder	All	All	All	All

References

Reference	Source	Link
File must be escaped as well to prevent XSS · ZoneMinder/zoneminder@d289eb4 · GitHub	MISC	github
Stored Cross-Site Script Vulnerability In File Parameter · Advisory · ZoneMinder/zoneminder · GitHub	CONFIRM	github
Zoneminder Log Injection / XSS / Cross Site Request Forgery ≈ Packet Storm	MISC	packe
Only perform actions on post. Doing them on GET allows doing actions ... · ZoneMinder/zoneminder@c0a4c05 · GitHub	MISC	github
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183581 Debian Security Update for zoneminder (CVE-2022-39285)

502977 Alpine Linux Security Update for zoneminder

505044 Alpine Linux Security Update for zoneminder

© [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](#)