



CVE-2022-39289

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

Summary

CVE	CVE-2022-39289
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	2023-07-14 18:13:00 UTC
Description	ZoneMinder is a free, open source Closed-circuit television software application. In affected versions the ZoneMinder API E

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
API Exposes Database Log contents to user without privileges, allows insertion, modification, deletion of logs without System Privileges · Advi
Add permissions checking to API/Logs. Fixes unprivileged user being t... · ZoneMinder/zoneminder@34ffd92 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502977](#) Alpine Linux Security Update for zoneminder

[505844](#) 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](#)