



CVE-2022-24716

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

Summary

CVE	CVE-2022-24716
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-08 20:15:00 UTC
Updated	2023-04-10 20:15:00 UTC
Description	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Unauthenticated users c

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icinga	Icinga Web 2	All	All	All	All

References

Reference	Source	Link
Icinga Web 2.10 Arbitrary File Disclosure ~ Packet Storm	MISC	packetstormsecu
Icinga Web 2: Multiple Vulnerabilities (GLSA 202208-05) — Gentoo security	GENTOO	security.gentoo.or
Merge pull request from GHSA-5p3f-rh28-8frw · Icinga/icingaweb2@9931ed7 · GitHub	MISC	github.com
Path traversal in static library file requests for unauthenticated users · Advisory · Icinga/icingaweb2 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183632](#) Debian Security Update for icingaweb2 (CVE-2022-24716)

[710576](#) Gentoo Linux Icinga Web 2 Multiple Vulnerabilities (GLSA 202208-05)

© [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](#)