



Ignite Realtime Openfire Path Traversal Vulnerability

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

Summary

CVE	CVE-2023-32315
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-26 23:15:00 UTC
Updated	2023-07-21 19:21:00 UTC
Description	Openfire is an XMPP server licensed under the Open Source Apache License. Openfire's administrative console, a web-ba

Risk And Classification

EPSS: 0.944410000 probability, percentile 0.999910000 (date 2026-04-02)

CISA KEV: Listed on 2023-08-24; due 2023-09-14; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Ignite Realtime
Product	Openfire
Name	Ignite Realtime Openfire Path Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://www.igniterealtime.org/downloads/#openfire ; https://nvd.nist.gov/vuln/detail/CVE-2023-32315

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	All	All	All	All

References

Reference	Source	Link	Tags
Administration Console authentication bypass · Advisory · igniterealtime/Openfire · GitHub	MISC	github.com	
Openfire Authentication Bypass / Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150722](#) Openfire Path Traversal Vulnerability (CVE-2023-32315)

[503205](#) Alpine Linux Security Update for openfire

[506134](#) Alpine Linux Security Update for openfire

[730838](#) Openfire Authentication Bypass Vulnerability (GHSA-gw42-f939-fhvm)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report