



CVE-2008-6508

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

Summary

CVE	CVE-2008-6508
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-23 20:00:00 UTC
Updated	2018-10-11 20:57:00 UTC
Description	Directory traversal vulnerability in the AuthCheck filter in the Admin Console in Openfire 3.6.0a and earlier allows remote at



Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	2.6.0	All	All	All
Application	Igniterealtime	Openfire	2.6.1	All	All	All
Application	Igniterealtime	Openfire	2.6.2	All	All	All
Application	Igniterealtime	Openfire	3.0.0	All	All	All
Application	Igniterealtime	Openfire	3.0.1	All	All	All
Application	Igniterealtime	Openfire	3.1.0	All	All	All
Application	Igniterealtime	Openfire	3.1.1	All	All	All
Application	Igniterealtime	Openfire	3.2.0	All	All	All
Application	Igniterealtime	Openfire	3.2.1	All	All	All
Application	Igniterealtime	Openfire	3.2.2	All	All	All
Application	Igniterealtime	Openfire	3.2.3	All	All	All
Application	Igniterealtime	Openfire	3.2.4	All	All	All
Application	Igniterealtime	Openfire	3.3.0	All	All	All
Application	Igniterealtime	Openfire	3.3.2	All	All	All
Application	Igniterealtime	Openfire	3.3.3	All	All	All
Application	Igniterealtime	Openfire	3.4.0	All	All	All
Application	Igniterealtime	Openfire	3.4.1	All	All	All

Application	Igniterealtime	Openfire	3.4.3	All	All	All
Application	Igniterealtime	Openfire	3.4.4	All	All	All
Application	Igniterealtime	Openfire	3.4.5	All	All	All
Application	Igniterealtime	Openfire	3.5.0	All	All	All
Application	Igniterealtime	Openfire	3.5.1	All	All	All
Application	Igniterealtime	Openfire	3.5.2	All	All	All
Application	Igniterealtime	Openfire	3.6.0	All	All	All
Application	Igniterealtime	Openfire	2.6.0	All	All	All
Application	Igniterealtime	Openfire	2.6.1	All	All	All
Application	Igniterealtime	Openfire	2.6.2	All	All	All
Application	Igniterealtime	Openfire	3.0.0	All	All	All
Application	Igniterealtime	Openfire	3.0.1	All	All	All
Application	Igniterealtime	Openfire	3.1.0	All	All	All
Application	Igniterealtime	Openfire	3.1.1	All	All	All
Application	Igniterealtime	Openfire	3.2.0	All	All	All
Application	Igniterealtime	Openfire	3.2.1	All	All	All
Application	Igniterealtime	Openfire	3.2.2	All	All	All
Application	Igniterealtime	Openfire	3.2.3	All	All	All
Application	Igniterealtime	Openfire	3.2.4	All	All	All
Application	Igniterealtime	Openfire	3.3.0	All	All	All
Application	Igniterealtime	Openfire	3.3.2	All	All	All
Application	Igniterealtime	Openfire	3.3.3	All	All	All
Application	Igniterealtime	Openfire	3.4.0	All	All	All
Application	Igniterealtime	Openfire	3.4.1	All	All	All
Application	Igniterealtime	Openfire	3.4.3	All	All	All
Application	Igniterealtime	Openfire	3.4.4	All	All	All
Application	Igniterealtime	Openfire	3.4.5	All	All	All
Application	Igniterealtime	Openfire	3.5.0	All	All	All
Application	Igniterealtime	Openfire	3.5.1	All	All	All
Application	Igniterealtime	Openfire	3.5.2	All	All	All
Application	Igniterealtime	Openfire	3.6.0	All	All	All
Application	Igniterealtime	Openfire	All	All	All	All

References						
Reference					Source	Link
10000					CC BY-SA	

49663	OSVDB	OSV
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	WV
SecurityFocus	BUGTRAQ	WV
Openfire Multiple Input Validation Vulnerabilities	BID	WV
[#JM-1489] Authentication bypass allowing arbitrary code execution - Jive Software Open Source	CONFIRM	WV
IBM X-Force Exchange	XF	ex
Andreas Kurtz » Blog Archiv » Openfire: Multiple Critical Vulnerabilities	MISC	WV
Openfire Server <= 3.6.0a (Auth Bypass/SQL/XSS) Multiple Vulnerabilities	EXPLOIT-DB	WV
Openfire Changelog	CONFIRM	WV
Openfire "AuthCheck" Filter Security Bypass Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	se
404 Page not found Dr. Andreas Kurtz	MISC	WV
CVE Program record	CVE.ORG	WV
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)