



CVE-2012-4889

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

Summary

CVE	CVE-2012-4889
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-10 22:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in ManageEngine Firewall Analyzer 7.2 allow remote attackers to inject ar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Manageengine	Firewall Analyzer	7.2	All	All	All
Application	Manageengine	Firewall Analyzer	7.2	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange
ME Firewall Analyzer 7.2 Cross Site Scripting ≈ Packet Storm	MISC	packetsto
80873	OSVDB	osvdb.org
80874	OSVDB	osvdb.org
Security Advisory SA48657 - ManageEngine Firewall Analyzer Multiple Cross-Site Scripting Vulnerabilities - Secunia	SECUNIA	secunia.c
80875	OSVDB	osvdb.org
80872	OSVDB	osvdb.org
Firewall Analyzer Multiple Cross Site Scripting Vulnerabilities	BID	www.seci
403 Forbidden	MISC	www.vuln
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)