



CVE-2014-7850

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

Summary

CVE	CVE-2014-7850
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-28 15:59:00 UTC
Updated	2015-02-17 14:36:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Web UI in FreeIPA 4.x before 4.1.2 allows remote attackers to inject arbitrary

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeipa	Freeipa	4.0.0	All	All	All
Application	Freeipa	Freeipa	4.0.1	All	All	All
Application	Freeipa	Freeipa	4.0.2	All	All	All
Application	Freeipa	Freeipa	4.0.3	All	All	All
Application	Freeipa	Freeipa	4.0.4	All	All	All
Application	Freeipa	Freeipa	4.0.5	All	All	All
Application	Freeipa	Freeipa	4.1.0	All	All	All
Application	Freeipa	Freeipa	4.1.1	All	All	All
Application	Freeipa	Freeipa	4.0.0	All	All	All
Application	Freeipa	Freeipa	4.0.1	All	All	All
Application	Freeipa	Freeipa	4.0.2	All	All	All
Application	Freeipa	Freeipa	4.0.3	All	All	All
Application	Freeipa	Freeipa	4.0.4	All	All	All
Application	Freeipa	Freeipa	4.0.5	All	All	All
Application	Freeipa	Freeipa	4.1.0	All	All	All
Application	Freeipa	Freeipa	4.1.1	All	All	All

References

Reference	Source	Link	Ta
#4742 (user input in breadcrumb navigation is not escaped) – freeipa	CONFIRM	fedorahosted.org	Ve
1165280 – (CVE-2014-7850) CVE-2014-7850 freeipa: XSS flaw can be used to escalate privileges	CONFIRM	bugzilla.redhat.com	Ve
[SECURITY] Fedora 21 Update: freeipa-4.1.1-2.fc21	FEDORA	lists.fedoraproject.org	Ve
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

© [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](https://www.mitre.org/licenses).

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