



CVE-2012-6133

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

Summary

CVE	CVE-2012-6133
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-30 21:15:00 UTC
Updated	2020-01-31 20:48:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in Roundup before 1.4.20 allow remote attackers to inject arbitrary web sc

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Roundup-tracker	Roundup	All	All	All	All
Application	Roundup-tracker	Roundup	All	All	All	All

References

Reference

Issue 2550724: XSS vulnerability in ok_message handling - Roundup tracker
oss-security - CVE Request -- roundup: Multiple XSS flaws plus other security related fixes corrected in upstream 1.4.20 version
722672 – (CVE-2012-6130, CVE-2012-6131, CVE-2012-6132) CVE-2012-6130 CVE-2012-6131 CVE-2012-6132 roundup: Multiple cross-site
roundup 1.4.20 : Python Package Index
oss-security - Re: CVE Request -- roundup: Multiple XSS flaws plus other security related fixes corrected in upstream 1.4.20 version
CVE Program record
NVD vulnerability detail

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](#)