



CVE-2012-2251

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2012-2251
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-11 01:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	rssh 2.3.2, as used by Debian, Fedora, and others, when the rsync protocol is enabled, allows local users to bypass intended

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Fedoraproject	Fedora	All	All	All	All
Operating System	Fedoraproject	Fedora	All	All	All	All
Application	Pizzashack	Rssh	2.3.2	All	All	All
Application	Pizzashack	Rssh	2.3.2	All	All	All

References

Reference	Source	Link
20121127 Re: rssh security announcement	BUGTRAQ	archives.neohapsis.com
About Secunia Research Flexera	SECUNIA	secunia.com
Debian -- Security Information -- DSA-2578-1 rssh	DEBIAN	www.debian.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
oss-security - rssh: incorrect filtering of command line options	MLIST	www.openwall.com
877279 – CVE-2012-2251 rssh: insufficient filtering of -e option for rsync [fedora-all]	CONFIRM	bugzilla.redhat.com
rssh Command Line Filtering Multiple Remote Arbitrary Command Execution Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org

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](#)