



CVE-2012-5536

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

Summary

CVE	CVE-2012-5536
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-22 00:55:00 UTC
Updated	2019-04-22 17:48:00 UTC
Description	A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Linux (RHEL) 6 and Fedora Rawhide co

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedora Project	Fedora Release Rawhide	-	All	All	All
Operating System	Fedora Project	Fedora Release Rawhide	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

References

Reference	Source	Link
Page not found :(- src.fedoraproject.org	CONFIRM	pkg
Red Hat Customer Portal	REDHAT	rhn
834618 – (CVE-2012-5536) CVE-2012-5536 pam_ssh_agent_auth: symbol crash leading to glibc error() called incorrectly	CONFIRM	bug
CVE Program record	CVE.ORG	www
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](#)