



CVE-2015-3983

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

Summary

CVE	CVE-2015-3983
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-14 14:59:00 UTC
Updated	2016-12-31 02:59:00 UTC
Description	The pcs daemon (pcsd) in PCS 0.9.137 and earlier does not include the HTTPOnly flag in a Set-Cookie header, which mak

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedora	Pacemaker Configuration System	All	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
bugzilla.redhat.com/attachment.cgi	CONFIRM	bugzilla.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
[SECURITY] Fedora 22 Update: pcs-0.9.139-4.fc22	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 20 Update: pcs-0.9.115-3.fc20	FEDORA	lists.fedoraproject.org	
pcs daemon CVE-2015-3983 Remote Information Disclosure Vulnerability	BID	www.securityfocus.com	
[SECURITY] Fedora 21 Update: pcs-0.9.137-4.fc21	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)