



CVE-2018-1086

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-1086
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-12 16:29:00 UTC
Updated	2019-10-09 23:38:00 UTC
Description	pcs before versions 0.9.164 and 0.10 is vulnerable to a debug parameter removal bypass. REST interface of the pcsd servi

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Pacemaker Command Line Interface	0.10	All	All	All
Application	Clusterlabs	Pacemaker Command Line Interface	0.9.164	All	All	All
Application	Clusterlabs	Pacemaker Command Line Interface	0.10	All	All	All
Application	Clusterlabs	Pacemaker Command Line Interface	0.9.164	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.r
Debian -- Security Information -- DSA-4169-1 pcs	DEBIAN	www.del
1557366 – (CVE-2018-1086) CVE-2018-1086 pcs: Debug parameter removal bypass, allowing information disclosure	MISC	bugzilla.
Red Hat Customer Portal	REDHAT	access.r

CVE Program record

CVE.ORG www.cve.org

NVD vulnerability detail

NVD nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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