



CVE-2018-16877

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

Summary

CVE	CVE-2018-16877
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-18 18:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	A flaw was found in the way pacemaker's client-server authentication was implemented in versions up to and including 2.0.0

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Application	Clusterlabs	Pacemaker	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All

References

Reference

[security-announce] openSUSE-SU-2019:1342-1: important: Security update

[SECURITY] Fedora 29 Update: pacemaker-2.0.0-5.fc29 - package-announce - Fedora Mailing-Lists

[security-announce] openSUSE-SU-2019:1400-1: important: Security update

[SECURITY] Fedora 29 Update: pacemaker-2.0.0-5.fc29 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2519-1] pacemaker security update

[SECURITY] Fedora 28 Update: pacemaker-1.1.18-3.fc28 - package-announce - Fedora Mailing-Lists

1652646 – (CVE-2018-16877) CVE-2018-16877 pacemaker: Insufficient local IPC client-server authentication on the client's side can lead to I

[SECURITY] Fedora 30 Update: pacemaker-2.0.1-2.fc30 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

Malformed Request

Pacemaker: Multiple Vulnerabilities (GLSA 202309-09) — Gentoo security

High: cumulative patchset to fix CVE-2019-3885, CVE-2018-16877, CVE-2018-16878 + additional unmasked null pointer deref by jnpkrn · Pull

Red Hat Customer Portal

USN-3952-1: Pacemaker vulnerabilities | Ubuntu security notices | Ubuntu

[SECURITY] Fedora 28 Update: pacemaker-1.1.18-3.fc28 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 30 Update: pacemaker-2.0.1-2.fc30 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)