



CVE-2013-0281

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

Summary

CVE	CVE-2013-0281
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-23 11:55:00 UTC
Updated	2019-04-22 17:48:00 UTC
Description	Pacemaker 1.1.10, when remote Cluster Information Base (CIB) configuration or resource management is enabled, does not

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Pacemaker	1.1.10	All	All	All
Application	Clusterlabs	Pacemaker	1.1.10	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
High: core: Internal tls api improvements for reuse with future LRMD ... · ClusterLabs/pacemaker@564f7cc · GitHub	CONFIRM
Red Hat Customer Portal	REDHAT
Bug 891922 – CVE-2013-0281 pacemaker: remote DoS when CIB management is enabled caused by use of blocking sockets	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	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](#).

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