



CVE-2017-1000406

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

Summary

CVE	CVE-2017-1000406
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-30 21:29:00 UTC
Updated	2017-12-20 18:52:00 UTC
Description	OpenDaylight Karaf 0.6.1-Carbon fails to clear the cache after a password change, allowing the old password to be used ur

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opendaylight	Karaf	0.6.1-carbon	All	All	All
Application	Opendaylight	Karaf	0.6.1-carbon	All	All	All

References

Reference

oss-sec: OpenDayLight: Password change doesn't result in Karaf clearing cache, allowing old password to still be used (CVE-2017-1000406)

Gerrit Code Review

[AAA-151] Previous password continues to work after password change - OpenDaylight JIRA

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

996911 Java (Maven) Security Update for org.opendaylight.integration:distribution-karaf (GHSA-4px2-gqhv-mrc7)

© [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](#)