



CVE-2012-6119

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

Summary

CVE	CVE-2012-6119
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-02 22:55:00 UTC
Updated	2013-04-03 04:00:00 UTC
Description	Candlepin before 0.7.24, as used in Red Hat Subscription Asset Manager before 1.2.1, does not properly check manifest si

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Candlepinproject	Candlepin	0.4.11	All	All	All
Application	Candlepinproject	Candlepin	0.4.27	All	All	All
Application	Candlepinproject	Candlepin	0.4.5	All	All	All
Application	Candlepinproject	Candlepin	0.5.5	All	All	All
Application	Candlepinproject	Candlepin	0.6.3	All	All	All
Application	Candlepinproject	Candlepin	All	All	All	All
Application	Candlepinproject	Candlepin	0.4.11	All	All	All
Application	Candlepinproject	Candlepin	0.4.27	All	All	All
Application	Candlepinproject	Candlepin	0.4.5	All	All	All
Application	Candlepinproject	Candlepin	0.5.5	All	All	All
Application	Candlepinproject	Candlepin	0.6.3	All	All	All
Application	Redhat	Subscription Asset Manager	1.0.0	All	All	All
Application	Redhat	Subscription Asset Manager	1.1.0	All	All	All
Application	Redhat	Subscription Asset Manager	1.0.0	All	All	All
Application	Redhat	Subscription Asset Manager	1.1.0	All	All	All
Application	Redhat	Subscription Asset Manager	All	All	All	All

References

Reference	Source	Link	Tags
Page not found · GitHub · GitHub	CONFIRM	github.com	
908613 – (CVE-2012-6119) CVE-2012-6119 Candlepin: Re-enable manifest signature checking	MISC	bugzilla.redhat.com	
91719	OSVDB	www.osvdb.org	
835977: Re-enable manifest signature checking. · candlepin/candlepin@f4d9323 · GitHub	CONFIRM	github.com	
Security Advisory SA52774 - Red Hat update for Red Hat Subscription Asset Manager - Secunia	SECUNIA	secunia.com	Vendo
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Vendo
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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

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

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