



CVE-2012-2328

Published on: 02/10/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:24 AM UTC

CVE-2012-2328

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Opensuse](#) from [Opensuse](#) contain the following vulnerability:

internal/cimxml/sax/NodeFactory.java in Standards-Based Linux Instrumentation for Manageability (SBLIM) Common Information Model (CIM) Client (aka sblim-cim-client2) before 2.1.12 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted XML file.

CVE-2012-2328 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

openSUSE-SU-2013:0144-1: moderate:
update for sblim-cim-client2

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2013:0144](#)

openSUSE-SU-2012:1621-1: moderate:
update for sblim-cim-client2

[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2012:1621](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[REDHAT RHSA-2012:0987](#)

CVS Info for project sblim

[sblim.cvs.sourceforge.net](#)
[text/html](#)

[MISC sblim.cvs.sourceforge.net/viewvc/sblim/jsr48-client/src/org/sblim/cimclient/internal/cimxml/sax/NodeFactory.java?view=log#rev1.7](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Application	Standards Based Linux Instrumentation Project	Standards-based Linux Common Information Model Client	All	All	All	All
cpe:2.3:o:opensuse:opensuse:11.4:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:opensuse:12.1:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:opensuse:12.2:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:opensuse:11.4:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:opensuse:12.1:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:opensuse:opensuse:12.2:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:standards_based_linux_instrumentation_project:standards-based_linux_common_information_model_client:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)