



CVE-2013-4221

Published on: 10/09/2013 12:00:00 AM UTC

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

CVE-2013-4221

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The default configuration of the `ObjectRepresentation` class in Restlet before 2.1.4 deserializes objects from untrusted sources using the Java `XMLDecoder`, which allows remote attackers to execute arbitrary Java code via crafted XML.

CVE-2013-4221 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

SECURITY: remote code execution due to XML deserialization in Restlet · Issue #774 · restlet/restlet-framework-java · GitHub

[Issue Tracking](#)
[Patch](#)
[github.com](#)
[text/html](#)

[CONFIRM](#)
github.com/restlet/restlet-framework-java/issues/774

Red Hat Customer Portal

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

[REDHAT RHSA-2013:1410](#)

Dinis Cruz Blog: Using XMLDecoder to execute server-side Java Code on an Restlet application (i.e. Remote Command Execution)

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

[MISC](#)
blog.diniscruz.com/2013/08/using-xmldecoder-to-execute-server-side.html

Red Hat Customer Portal

[Third Party Advisory](#)
[web.archive.org](#)

[REDHAT RHSA-2013:1862](#)

restlet.org
text/html
Inactive Link Not Archived

Talend - A Cloud Data Integration Leader (modern ETL)

Release Notes
Vendor Advisory
restlet.org
text/plain

 CONFIRM
restlet.org/learn/2.1/changes

995275 – (CVE-2013-4221) CVE-2013-4221 Restlet: remote code execution due to insecure XML deserialization

Issue Tracking
Third Party Advisory
bugzilla.redhat.com
text/html

 CONFIRM
bugzilla.redhat.com/show_bug.cgi?id=995275

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
Application	Restlet	Restlet	2.1	milestone1	All	All
Application	Restlet	Restlet	2.1	milestone2	All	All
Application	Restlet	Restlet	2.1	milestone3	All	All
Application	Restlet	Restlet	2.1	milestone4	All	All
Application	Restlet	Restlet	2.1	milestone5	All	All
Application	Restlet	Restlet	2.1	milestone6	All	All
Application	Restlet	Restlet	2.1	rc1	All	All
Application	Restlet	Restlet	2.1	rc2	All	All
Application	Restlet	Restlet	2.1	rc3	All	All
Application	Restlet	Restlet	2.1	rc4	All	All
Application	Restlet	Restlet	2.1	rc5	All	All
Application	Restlet	Restlet	2.1	rc6	All	All
Application	Restlet	Restlet	2.1.0	All	All	All
Application	Restlet	Restlet	2.1.1	All	All	All
Application	Restlet	Restlet	2.1.2	All	All	All
Application	Restlet	Restlet	2.1	milestone1	All	All
Application	Restlet	Restlet	2.1	milestone2	All	All
Application	Restlet	Restlet	2.1	milestone3	All	All
Application	Restlet	Restlet	2.1	milestone4	All	All
Application	Restlet	Restlet	2.1	milestone5	All	All
Application	Restlet	Restlet	2.1	milestone6	All	All

Application	Restlet	Restlet	2.1	rc1	All	All
Application	Restlet	Restlet	2.1	rc2	All	All
Application	Restlet	Restlet	2.1	rc3	All	All
Application	Restlet	Restlet	2.1	rc4	All	All
Application	Restlet	Restlet	2.1	rc5	All	All
Application	Restlet	Restlet	2.1	rc6	All	All
Application	Restlet	Restlet	2.1.0	All	All	All
Application	Restlet	Restlet	2.1.1	All	All	All
Application	Restlet	Restlet	2.1.2	All	All	All
Application	Restlet	Restlet	All	All	All	All
cpe:2.3:a:restlet:restlet:2.1:milestone1:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone2:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone3:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone4:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone5:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone6:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc1:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc2:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc3:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc4:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc5:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:rc6:*****:~:						
cpe:2.3:a:restlet:restlet:2.1.0:*****:~:						
cpe:2.3:a:restlet:restlet:2.1.1:*****:~:						
cpe:2.3:a:restlet:restlet:2.1.2:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone1:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone2:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone3:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone4:*****:~:						
cpe:2.3:a:restlet:restlet:2.1:milestone5:*****:~:						

cpe:2.3:a:restlet:restlet:2.1:milestone6:*****:
cpe:2.3:a:restlet:restlet:2.1:rc1:*****:
cpe:2.3:a:restlet:restlet:2.1:rc2:*****:
cpe:2.3:a:restlet:restlet:2.1:rc3:*****:
cpe:2.3:a:restlet:restlet:2.1:rc4:*****:
cpe:2.3:a:restlet:restlet:2.1:rc5:*****:
cpe:2.3:a:restlet:restlet:2.1:rc6:*****:
cpe:2.3:a:restlet:restlet:2.1.0:*****:
cpe:2.3:a:restlet:restlet:2.1.1:*****:
cpe:2.3:a:restlet:restlet:2.1.2:*****:
cpe:2.3:a:restlet:restlet:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)