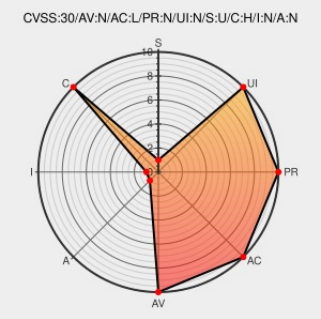
CVE-2017-14949

Published on: 11/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14949

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Restlet from Restlet contain the following vulnerability:

Restlet Framework before 2.3.12 allows remote attackers to access arbitrary files via a crafted REST API HTTP request that conducts an XXE attack, because only general external entities (not parameter external entities) are properly considered. This is related to XmlRepresentation, DOMRepresentation, SaxRepresentation, and JacksonRepresentation.

CVE-2017-14949 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Parameter entity XXE vulnerability in Restlet (CVE-2017-14949) - Blog - LGTM	Exploit, Third Party Advisory	MISC lgtm.com/blog/restlet_CVE-2017-14949

	web.archive.org text/html Inactive Link Not Archived	
XEE security enhancements · restlet/restlet-framework-java Wiki · GitHub	Third Party Advisory github.com text/html	MISC github.com/restlet/restlet-framework-java/wiki/XEE-security-enhancements

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.

Related QID Numbers

983769 Java (maven) Security Update for org.restlet.jse:org.restlet (GHSA-cvj4-g3gx-8vqq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Restlet	Restlet	All	All	All	All
Application	Restlet	Restlet	All	All	All	All

cpe:2.3:a:restlet:restlet:*:*:*:*:*:*:*:*:

cpe:2.3:a:restlet:restlet:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→