



CVE-2022-40705

Published on: Not Yet Published

Last Modified on: 09/24/2022 02:36:00 AM UTC

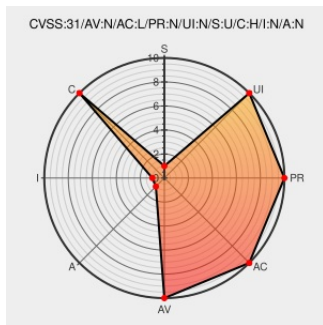
CVE-2022-40705

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Simple Object Access Protocol](#) from [Apache](#) contain the following vulnerability:

**** UNSUPPORTED WHEN ASSIGNED **** An Improper Restriction of XML External Entity Reference vulnerability in RPCRouterServlet of Apache SOAP allows an attacker to read arbitrary files over HTTP. This issue affects Apache SOAP version 2.2 and later versions. It is unknown whether previous versions are also affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2022-40705 has been assigned by security@apache.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache SOAP** version **>= 2.2**

Affected Vendor/Software: **Apache Software Foundation - Apache SOAP** version **? < 2.2**

Vulnerability Patch/Work Around

We do not expect to release a version that fixes this problem. Instead, we recommend users to migrate to one of the other actively maintained web service stacks such as Apache CXF (<https://cxf.apache.org>) or Apache Axis (<https://axis.apache.org>). Apache SOAP is an archived project, with the last release published in 2003. This means it is no longer maintained, does not receive updates, and we do not commit to publishing CVE's for security problems in this project. This advisory is published purely as a courtesy.

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

CVE References

Description	Tags	Link

No Description Provided

[lists.apache.org](https://lists.apache.org/text/html)
text/html

MISC
lists.apache.org/thread/02yo04w93rdjmlz4454lvodn5xzhwhl

oss-security - CVE-2022-40705: Apache SOAP: XML External Entity Injection (XXE) allows unauthenticated users to read arbitrary files via HTTP

[www.openwall.com](https://www.openwall.com/text/html)
text/html

MLIST [oss-security] 20220922 CVE-2022-40705: Apache SOAP: XML External Entity Injection (XXE) allows unauthenticated users to read arbitrary files via HTTP

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	Apache	Simple Object Access Protocol	All	All	All	All
<code>cpe:2.3:a:apache:simple_object_access_protocol:*:*:*:*:*:*</code>						

Discovery Credit

Apache would like to thank TsungShu Chiu (CHT Security) for reporting this issue

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-40705 : An Improper Restriction of XML External Entity Reference vulnerability in RPCRouterServlet of... twitter.com/i/web/status/1...	2022-09-22 08:17:28
@Inceptus3	New Vulnerability: CVE-2022-40705 #InceptusSecure #UnderOurProtection	2022-09-22 10:15:22
/r/netcve	CVE-2022-40705	2022-09-22 09:38:20

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

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](#).

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