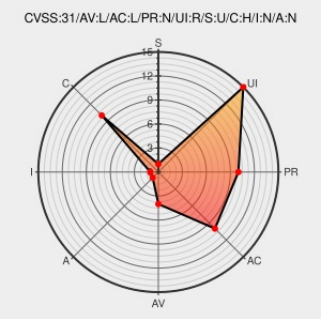
CVE-2019-17554

Published on: 12/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:38 PM UTC

CVE-2019-17554

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



Certain versions of Olingo from Apache contain the following vulnerability:

The XML content type entity deserializer in Apache Olingo versions 4.0.0 to 4.6.0 is not configured to deny the resolution of external entities. Request with content type "application/xml", which trigger the deserialization of entities, can be used to trigger XXE attacks.

CVE-2019-17554 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apache** - **Olingo** version **4.0.0 to 4.6.0**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Bugtraq: CVE-2019-17554 - Apache Olingo OData 4.0 - XML External Entity Resolution (XXE)	Exploit, Third Party Advisory, seclists.org	BUGTRAQ 20191210 CVE-2019-17554 - Apache Olingo OData 4.0 - XML External Entity Resolution (XXE)

	text/html	
Pony Mail!	lists.apache.org text/html	MLIST [announce] 20200131 Apache Software Foundation Security Report: 2019
[SECURITY] CVE-2019-17554: XML External Entity resolution attack	Mailing List Vendor Advisory mail-archives.apache.org text/xml	MLIST [olingo-user] 20191204 [SECURITY] CVE-2019-17554: XML External Entity resolution attack
Apache Olingo OData 4.6.x XML Injection ≈ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155619/Apache-Olingo-OData-4.6.x-XML-Injection.html

Related QID Numbers

981597 Java (maven) Security Update for org.apache.olingo:odata-server-core (GHSA-mgh8-hcwj-h57v)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Olingo	All	All	All	All

cpe:2.3:a:apache:olingo:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→