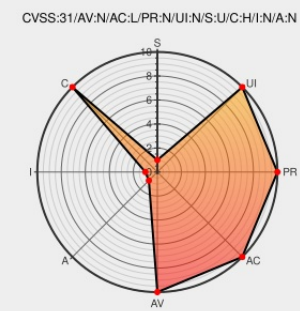
CVE-2020-26708

Published on: Not Yet Published

Last Modified on: 09/08/2023 05:15:00 PM UTC

CVE-2020-26708

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



Certain versions of Requests-xml from Requests-xml Project contain the following vulnerability:

requests-xml v0.2.3 was discovered to contain an XML External Entity Injection (XXE) vulnerability which allows attackers to execute arbitrary code via a crafted XML file.

CVE-2020-26708 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

CVE References

Description	Tags	Link
CVE-2020-26708 requests-xml Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20230908-0003/
XML External Entity (XXE) · Issue #7 · erinxocon/requests-xml · GitHub	github.com text/html	MISC github.com/erinxocon/requests-xml/issues/7

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Requests-xml Project	Requests-xml	0.2.3	All	All	All

cpe:2.3:a:requests-xml_project:requests-xml:0.2.3:*:*:*:*:python:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→