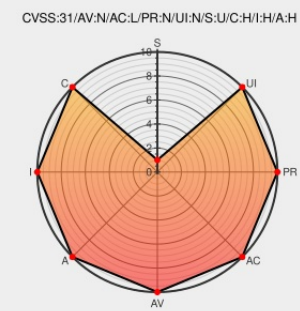
CVE-2022-35411

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-35411

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



Certain versions of Rpc.py from Rpc.py Project contain the following vulnerability:

rpc.py through 0.6.0 allows Remote Code Execution because an unpickle occurs when the "serializer: pickle" HTTP header is sent. In other words, although JSON (not Pickle) is the default data format, an unauthenticated client can cause the data to be processed with unpickle.

CVE-2022-35411 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
rpc.py 0.6.0 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167872/rpc.py-0.6.0-Remote-Code-Execution.html
GitHub - ehtec/rpcpy-exploit:	github.com	MISC github.com/ehtec/rpcpy-exploit

Unauthenticated Remote Code Execution for rpc.py server	text/html	
Remote Code Execution 0-day in rpc.py | by Elias Hohl | Jul, 2022 | Medium	medium.com text/html	MISC medium.com/@elias.hohl/remote-code-execution-0-day-in-rpc-py-709c76690c30
PickleSerializer is turned off by default · abersheeran/rpc.py@491e7a8 · GitHub	github.com text/html	MISC github.com/abersheeran/rpc.py/commit/491e7a841ed9a754796d6ab047a9fb16e23

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpc.py Project	Rpc.py	All	All	All	All

cpe:2.3:a:rpc.py_project:rpc.py:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Inceptus3	New Vulnerability: CVE-2022-35411 #InceptusSecure #UnderOurProtection	2022-07-08 20:12:13
/r/netcve	CVE-2022-35411	2022-07-08 19:38:18

← Previous ID

Next ID→

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