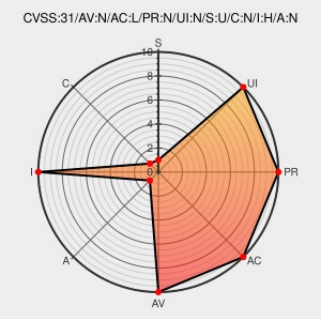
CVE-2019-16328

Published on: 10/03/2019 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:24:00 PM UTC

CVE-2019-16328

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



Certain versions of Rpyc from Rpyc Project contain the following vulnerability:

In RPyC 4.1.x through 4.1.1, a remote attacker can dynamically modify object attributes to construct a remote procedure call that executes code for an RPyC service with default configuration settings.

CVE-2019-16328 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	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
GitHub - tomerfiliba-org/rpyc: RPyC (Remote Python Call) - A transparent and symmetric RPC library for python	Product, Third Party Advisory, github.com, text/html	MISC github.com/tomerfiliba/rpyc

Security — RPyC	Exploit Vendor Advisory rpyc.readthedocs.io text/html	MISC rpyc.readthedocs.io/en/latest/docs/security.html
[security-announce] openSUSE-SU-2020:0685-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0685
[security-announce] openSUSE-SU-2020:0763-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0763

Related QID Numbers

980652 Python (pip) Security Update for rpyc (GHSA-pj4g-4488-wmxm)

982946 Python (pip) Security Update for rpyc (GHSA-9ggp-4jpr-7ppj)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpyc Project	Rpyc	All	All	All	All

cpe:2.3:a:rpyc_project:rpyc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→