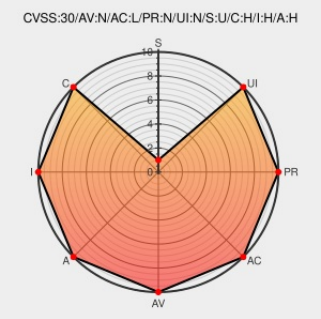
CVE-2017-16616

Published on: 11/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16616

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



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

An exploitable vulnerability exists in the YAML parsing functionality in the YAMLParser method in Interfaces.py in PyAnyAPI before 0.6.1. A YAML parser can execute arbitrary Python commands resulting in command execution because load is used where safe_load should have been used. An attacker can insert Python into loaded YAML to trigger this vulnerability.

CVE-2017-16616 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
CVE-2017-16616: YAMLParser in PyAnyAPI - Joel	Third Party Advisory joel-malwarebenchmark.github.io	MISC joel-malwarebenchmark.github.io/blog/2017/11/08/cve-

	text/html	2017-16616-yamlparser-in-pyanyapi/
YAMLParser method is vulnerable · Issue #41 · Stranger6667/pyanyapi · GitHub	Issue Tracking github.com text/html	CONFIRM github.com/Stranger6667/pyanyapi/issues/41
pyanyapi · PyPI	Product pypi.python.org text/html	CONFIRM pypi.python.org/pypi/pyanyapi/0.6.1
Release Release 0.6.1 · Stranger6667/pyanyapi · GitHub	Release Notes github.com text/html	CONFIRM github.com/Stranger6667/pyanyapi/releases/tag/0.6.1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:pyanyapi_project:pyanyapi:*:*:*:*:*:*:*:*:

cpe:2.3:a:pyanyapi_project:pyanyapi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→