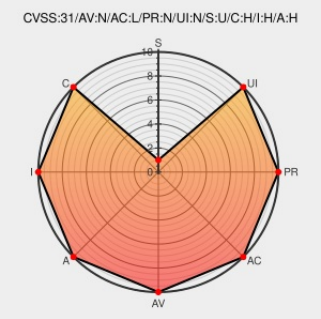
# CVE-2020-22083

Published on: 12/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:10 PM UTC

## CVE-2020-22083

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




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

** DISPUTED ** jsonpickle through 1.4.1 allows remote code execution during deserialization of a malicious payload through the decode() function. Note: It has been argued that this is expected and clearly documented behaviour. pickle is known to be capable of causing arbitrary code execution, and must not be used with un-trusted data.

CVE-2020-22083 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 |
|---|---|---|
| Jsonpickle decode() function unsafely form objects that can lead to Remote code execution · Issue #332 · jsonpickle/jsonpickle · GitHub | Third Party Advisory<br>github.com<br>text/html | MISC<br>github.com/jsonpickle/jsonpickle/issues/332#issuecomment-747807494 |

| | | |
|---|---|---|
| GitHub - j0lt-github/python-deserialization-attack-payload-generator: Peas create serialized payload for deserialization RCE attack on python driven applications where pickle ,pyYAML, ruamel.yaml or jsonpickle module is used for deserialization of serialized data. I will update it with more attack vectors to targets other modules. | Third Party Advisory<br>github.com<br>text/html | MISC github.com/j0lt-github/python-deserialization-attack-payload-generator |
| JSON Pickle Exploitation \| Python's Pickle Module - Target for Exploitation | Exploit<br>Third Party Advisory<br>versprite.com<br>text/html | MISC versprite.com/blog/application-security/into-the-jar-jsonpickle-exploitation/ |
| Jsonpickle decode() function unsafely form objects that can lead to Remote code execution · Issue #332 · jsonpickle/jsonpickle · GitHub | Third Party Advisory<br>github.com<br>text/html | MISC github.com/jsonpickle/jsonpickle/issues/332 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | Third Party Advisory<br>access.redhat.com<br>text/html | MISC access.redhat.com/security/cve/CVE-2020-22083 |
| jsonpickle 1.4.2 vulnerable to RCE · GitHub | Third Party Advisory<br>gist.github.com<br>text/html | MISC gist.github.com/j0lt-github/bb543e77a1a10c33cb56cf23d0837874 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Jsonpickle Project | Jsonpickle | All | All | All | All |

cpe:2.3:a:jsonpickle_project:jsonpickle:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→