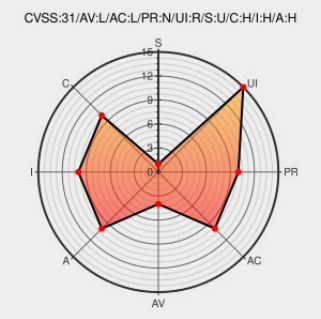
CVE-2021-35196

Published on: 06/21/2021 12:00:00 AM UTC

Last Modified on: 06/25/2021 12:59:00 PM UTC

CVE-2021-35196

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



Certain versions of Manuskript from Theologeek contain the following vulnerability:

** DISPUTED ** Manuskript through 0.12.0 allows remote attackers to execute arbitrary code via a crafted settings.pickle file in a project file, because there is insecure deserialization via the pickle.load() function in settings.py. NOTE: the vendor's position is that the product is not intended for opening an untrusted project file.

CVE-2021-35196 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Arbitrary Code Execution in Manuskript < 0.12 | Pizza Powered Hacking	www.pizzapower.me text/html	MISC www.pizzapower.me/2021/06/20/arbitrary-code-execution-in-manuskript-0-12/
Possible security issue · Issue #891 ·	github.com	MISC github.com/olivierkes/manuskript/issues/891

olivierkes/manuskript · GitHub

text/html

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.

Related QID Numbers

184883 Debian Security Update for manuskript (CVE-2021-35196)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theologeek	Manuskript	All	All	All	All

cpe:2.3:a:theologeek:manuskript:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-35196 : ** DISPUTED ** Manuskript through 0.12.0 allows remote attackers to execute arbitrary code via a c… twitter.com/i/web/status/1…	2021-06-21 23:07:47
/r/netcve	CVE-2021-35196	2021-06-21 23:41:40

← Previous ID

Next ID→