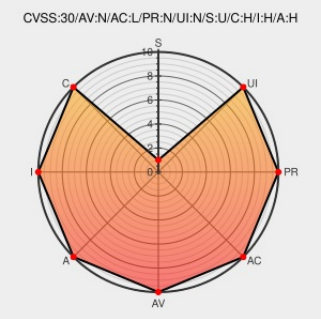
CVE-2017-16763

Published on: 11/10/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16763

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



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

An exploitable vulnerability exists in the YAML parsing functionality in config.py in Confire 0.2.0. Due to the user-specific configuration being loaded from "~/.confire.yaml" using the yaml.load function, a YAML parser can execute arbitrary Python commands resulting in command execution. An attacker can insert Python into loaded YAML to trigger this vulnerability.

CVE-2017-16763 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
load() method in class Configuration is vulnerable	Exploit, Third Party Advisory	MISC github.com/bbengfort/confire/issues/24

· Issue #24 · bbengfort/confire · GitHub	github.com text/html	
use safe load instead of load · bbengfort/confire@8cc86a5 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/bbengfort/confire/commit/8cc86a5ec2327e070f1d576d61bbaadf86
CVE-2017-16763: configure loaded through Confire - Joel	Exploit Third Party Advisory joel-malwarebenchmark.github.io text/html	MISC joel-malwarebenchmark.github.io/blog/2017/11/12/cve-2017-16763-configure-loaded-through-confire/

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

980993 Python (pip) Security Update for confire (GHSA-m85c-9mf8-m2m6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Confire Project	Confire	0.2.0	All	All	All
Application	Confire Project	Confire	0.2.0	All	All	All

cpe:2.3:a:confire_project:confire:0.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:confire_project:confire:0.2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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