



CVE-2016-3957

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-3957
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-06 18:29:00 UTC
Updated	2019-06-21 22:15:00 UTC
Description	The secure_load function in gluon/utils.py in web2py before 2.14.2 uses pickle.loads to deserialize session information stored in the database. This allows an attacker to execute arbitrary code with the privileges of the web2py process.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Web2py	Web2py	All	All	All	All
Application	Web2py	Web2py	All	All	All	All

References

Reference	Source	Link	Tags
WEB2PY 反序列化的安全問題 - CVE-2016-3957 DEVCORE 戴夫寇爾	MISC	devco.re	Exploit, Technical Description, Third Party Advisory
web2py/utils.py at R-2.14.1 · web2py/web2py · GitHub	MISC	github.com	Third Party Advisory
USN-4030-1: web2py vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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