



CVE-2018-14505

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

Summary

CVE	CVE-2018-14505
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-22 18:29:00 UTC
Updated	2018-09-18 13:23:00 UTC
Description	mitmweb in mitmproxy v4.0.3 allows DNS Rebinding attacks, related to tools/web/app.py.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mitmproxy	Mitmproxy	4.0.3	All	All	All
Application	Mitmproxy	Mitmproxy	4.0.3	All	All	All

References

Reference	Source	Link	Tags
mitmweb: protect against dns rebinding by mhils · Pull Request #3243 · mitmproxy/mitmproxy · GitHub	CONFIRM	github.com	Third Party
mitmweb isn't protected against DNS rebinding · Issue #3234 · mitmproxy/mitmproxy · GitHub	CONFIRM	github.com	Exploit, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981265](#) Python (pip) Security Update for mitmproxy (GHSA-6m53-c78q-7qmg)

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