



CVE-2021-39214

Published on: 09/16/2021 12:00:00 AM UTC

Last Modified on: 09/28/2021 02:21:00 PM UTC

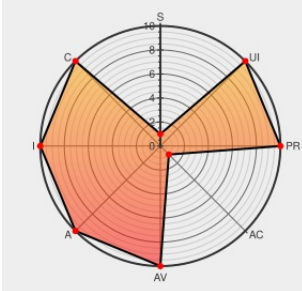
CVE-2021-39214 - advisory for GHSA-22gh-3r9q-xf38

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Mitmproxy](#) from [Mitmproxy](#) contain the following vulnerability:

mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.2 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While a smuggled request is still captured as part of another request's body, it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless one uses mitmproxy to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 7.0.3 and above.

CVE-2021-39214 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **mitmproxy** - mitmproxy version < 7.0.3

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
Lacking Protection against HTTP Request Smuggling in mitmproxy · Advisory · mitmproxy/mitmproxy · GitHub	github.com text/html	 CONFIRM github.com/mitmproxy/mitmproxy/security/advisories/GHSA-22gh-3r9q-xf38

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



980381 Python (pip) Security Update for mitmproxy (GHSA-22gh-3r9q-xf38)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mitmproxy	Mitmproxy	All	All	All	All
cpe:2.3:a:mitmproxy:mitmproxy:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-39214 : mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.2 and below, a m... twitter.com/i/web/status/1...	2021-09-16 15:13:11
 @threatmeter	CVE-2021-39214 mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.2 and below, a mal... twitter.com/i/web/status/1...	2021-09-17 07:09:45

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)