



CVE-2022-31033

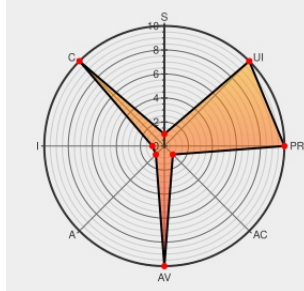
Published on: Not Yet Published

Last Modified on: 11/07/2023 03:47:00 AM UTC

CVE-2022-31033 - advisory for GHSA-64qm-hrgp-pgr9

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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



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

The Mechanize library is used for automating interaction with websites. Mechanize automatically stores and sends cookies, follows redirects, and can follow links and submit forms. In versions prior to 2.8.5 the Authorization header is leaked after a redirect to a different port on the same site. Users are advised to upgrade to Mechanize v2.8.5 or later.

There are no known workarounds for this issue.

CVE-2022-31033 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [sparklemotion](#) - **mechanize** version < 2.8.5

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
-------------	------	------

[SECURITY] Fedora 36 Update:
rubygem-mechanize-2.8.5-1.fc36 -
package-announce - Fedora
Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2022-6b1b324753

[SECURITY] Fedora 35 Update:
rubygem-mechanize-2.8.5-1.fc35 -
package-announce - Fedora
Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2022-fda14723ec

Merge pull request #600 from
sparklemotion/flavorjones-redirect-
headers ·
sparklemotion/mechanize@c7fe699
· GitHub

github.com
text/html

MISC
github.com/sparklemotion/mechanize/commit/c7fe6996a5b95f9880653ba3bc54

Authorization header leak on port
redirect · Advisory ·
sparklemotion/mechanize · GitHub

github.com
text/html

CONFIRM github.com/sparklemotion/mechanize/security/advisories/GHSA-6pgr9

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

182532 Debian Security Update for ruby-mechanize (CVE-2022-31033)

282847 Fedora Security Update for rubygem (FEDORA-2022-fda14723ec)

282848 Fedora Security Update for rubygem (FEDORA-2022-6b1b324753)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Mechanize Project	Mechanize	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:						
cpe:2.3:a:mechanize_project:mechanize:*:*:*:*:ruby:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31033 : The Mechanize library is used for automating interaction with websites. Mechanize automatically st... twitter.com/i/web/status/1...	2022-06-09 20:05:09

[← Previous ID](#)[Next ID→](#)© [CVE.report](#) 2023   |

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](#)