

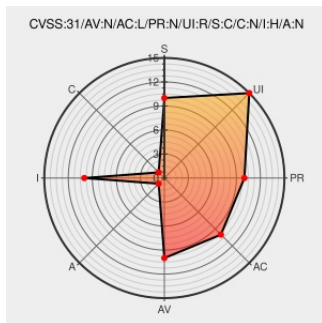


CVE-2021-21289

Published on: 02/02/2021 12:00:00 AM UTC

Last Modified on: 04/26/2022 03:07:00 PM UTC

CVE-2021-21289 - advisory for GHSA-qrqm-fpv6-6r8g

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

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

Mechanize is an open-source ruby library that makes automated web interaction easy. In Mechanize from version 2.0.0 and before version 2.7.7 there is a command injection vulnerability. Affected versions of mechanize allow for OS commands to be injected using several classes' methods which implicitly use Ruby's Kernel.open method.

Exploitation is possible only if untrusted input is used as a local filename and passed to any of these calls: Mechanize::CookieJar#load, Mechanize::CookieJar#save_as, Mechanize#download, Mechanize::Download#save, Mechanize::File#save, and Mechanize::FileResponse#read_body. This is fixed in version 2.7.7.

CVE-2021-21289 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: sparklemotion - mechanize version >= 2.0, < 2.7.7

CVSS3 Score: **8.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.6 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[SECURITY] [DLA 2561-1] ruby-mechanize security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20210216 [SECURITY] [DLA 2561-1] ruby-me security update
Merge pull request #548 from kyoshidajp/fix_command_injection · sparklemotion/mechanize@66a6a1b · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/sparklemotion/mechanize/commit/66a6a1bfa653a5f13274a396a5e5
Command Injection Vulnerability · Advisory · sparklemotion/mechanize · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/sparklemotion/mechanize/security/advisories/GHSA-4
Release 2.7.7 / 2021-02-01 · sparklemotion/mechanize · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/sparklemotion/mechanize/releases/tag/v2.7.7
Mechanize: Command injection (GLSA 202107-17) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202107-17
[SECURITY] Fedora 32 Update: rubygem-mechanize-2.7.7-1.fc32 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-24fdc228e4
[SECURITY] Fedora 33 Update: rubygem-mechanize-2.7.7-1.fc33 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-db8ebc547e
mechanize RubyGems.org your community gem host	Product Third Party Advisory rubygems.org text/html	 MISC rubygems.org/gems/mechanize/

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

[180101](#) Debian Security Update for ruby-mechanize (CVE-2021-21289)

[710059](#) Gentoo Linux Mechanize Command injection (GLSA 202107-17)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Mechanize Project	Mechanize	All	All	All	All
Application	Mechanize Project	Mechanize	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:a:mechanize_project:mechanize:*:*:*:*:ruby:*:						
cpe:2.3:a:mechanize_project:mechanize:*:*:*:*:ruby:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LinInfoSec	Ruby - CVE-2021-21289: rubygems.org/gems/mechanize/	2021-07-08 10:46:16
 @RemotelyAlerts	Severity: ??? Mechanize is an open-source ruby library... CVE-2021-21289 Link for more: alerts.remotelyrmm.com/CVE-2021-21289	2022-04-26 16:30:34
 @LinInfoSec	Ruby - CVE-2021-21289: rubygems.org/gems/mechanize/	2022-04-26 18:05:17

[← 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](#).

