



CVE-2021-32819

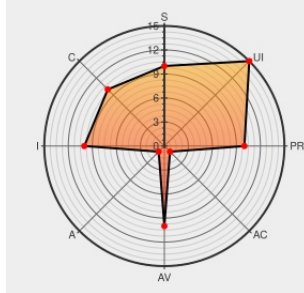
Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 05/22/2023 07:15:00 PM UTC

CVE-2021-32819 - advisory for GHSL-2021-023

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

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



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

Squirrelly is a template engine implemented in JavaScript that works out of the box with ExpressJS. Squirrelly mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options remote code execution may be triggered in downstream applications. This issue is fixed in version 9.0.0. For complete details refer to the referenced GHSL-2021-023.

CVE-2021-32819 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [squirrellyjs](#) - **squirrelly** version < 9.0.0

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

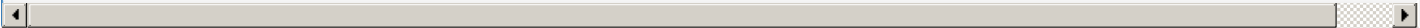
Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

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

don't pass view options · squirrellyjs/squirrelly@dca7a1e · GitHub	github.com text/html	MISC github.com/squirrellyjs/squirrelly/commit/dca7a1e7ee91d8a6ffffb655f3f15647486db9
GHSL-2021-023: Remote code execution in squirrelly - CVE-2021-32819 GitHub Security Lab	securitylab.github.com text/html	MISC securitylab.github.com/advisories/GHSL-2021-023-squirrelly/
Don't merge data.settings into the config option · squirrellyjs/squirrelly@c12418a · GitHub	github.com text/html	MISC github.com/squirrellyjs/squirrelly/commit/c12418a026f73df645ba927fd29358efe02fe
[security] Don't use data object for Squirrelly configuration by legobeat · Pull Request #254 · squirrellyjs/squirrelly · GitHub	github.com text/html	MISC github.com/squirrellyjs/squirrelly/pull/254
squirrelly - npm	www.npmjs.com text/html	MISC www.npmjs.com/package/squirrelly

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

982588 Nodejs (npm) Security Update for squirrelly (GHSA-q8j6-pwqx-pm96)

Exploit/POC from Github

SquirrellyJS mixes pure template data with engine configuration options through the Express render API. By overwritin...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squirrelly	Squirrelly	8.0.8	All	All	All
cpe:2.3:a:squirrelly:squirrelly:8.0.8-*.***:*.***:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2021-023: Remote code execution in squirrelly - CVE-2021-32819 github.co/3hEcH3d	2021-05-14 16:20:01
@CVEreport	CVE-2021-32819 : Squirrelly is a template engine implemented in JavaScript that works out of the box with ExpressJS... twitter.com/i/web/status/1...	2021-05-14 18:25:54
/r/netcve	CVE-2021-32819	2021-05-14 18:11:00

[← 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](#)