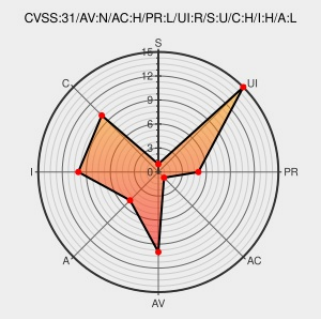
CVE-2020-15135

Published on: 08/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15135 - advisory for GHSA-wwrj-35w6-77ff

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Save-server from Save-server Project contain the following vulnerability:

save-server (npm package) before version 1.05 is affected by a CSRF vulnerability, as there is no CSRF mitigation (Tokens etc.). The fix introduced in version version 1.05 unintentionally breaks uploading so version v1.0.7 is the fixed version. This is patched by implementing Double submit. The CSRF attack would require you to navigate to a malicious site while you have an active session with Save-Server (Session key stored in cookies). The malicious user would then be able to perform some actions, including uploading/deleting files and adding redirects. If you are logged in as root, this attack is significantly more severe. They can in addition create, delete and update users. If they updated the password of a user, that user's files would then be available. If the root password is updated, all files would be visible if they logged in with the new password. Note that due to the same origin policy malicious actors cannot view the gallery or the response of any of the methods, nor be sure they succeeded. This issue has been patched in version 1.0.7.

CVE-2020-15135 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Neztore** - **save-server** version **< 1.0.5**

CVSS3 Score: 7.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	LOW

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Double Submit Cookie Pattern. Previously, I have discussed the… | by Harsha kavinda | cross-site-request-forgery-csrf | Medium	Exploit, Third Party Advisory, medium.com, text/html	MISC medium.com/cross-site-request-forgery-csrf/double-submit-cookie-pattern-65bb71d80d9f
CSRF vulnerability · Advisory · Neztore/save-server · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/Neztore/save-server/security/advisories/GHSA-wwrj-35w6-77ff
save-server - npm	Product, Third Party Advisory, www.npmjs.com, text/html	MISC www.npmjs.com/package/save-server

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

983195 Nodejs (npm) Security Update for save-server (GHSA-wwrj-35w6-77ff)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Save-server Project	Save-server	All	All	All	All
Application	Save-server Project	Save-server	All	All	All	All

cpe:2.3:a:save-server_project:save-server:*:*:*:*:*:node.js:*:*

cpe:2.3:a:save-server_project:save-server:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report