

Stored XSS in GlobalNewFiles (CVE-2021-39186)

Closed, ResolvedPublic

Actions

Assigned To

Majavah

Authored By

Majavah

2021-09-01 14:54:28 (UTC+0)

Tags

Security

(Backlog)

GlobalNewFiles

(Bugs)

Universal\_Omega

(Unsorted)

MediaWiki (SRE)

(Short Term)

Referenced Files

None

Subscribers

Majavah

Reception123

RhinosF1

Universal\_Omega

Void

Description

Steps to reproduce:

- Register a new account with the username " onclick=alert(document.domain)
- Upload a new file
- Visit Special:GlobalNewFiles (with a privileged account, if you want)
- Click on the username

Results:

- Clicking on the URL should lead into the user's CentralAuth page instead of executing JavaScript specified in the username

Recommended fix:

- Use MediaWiki's own helpers (Html, LinkRenderer, ...) instead of hand-crafting urls, apply htmlspecialchars() where necessary
  - Quick example:

```
case 'files_user':
-     $formatted = "<a href=\"/wiki/Special:CentralAuth/($row->files_user)\">{$row->files_user}</a>";
+     $formatted = MediaWikiServices::getInstance()->getLinkRenderer()->makeLink(
+         SpecialPage::getTitleFor( 'CentralAuth', $row->files_user ),
+         $row->files_user
+     );
+     break;
```

- Use static analysis tools such as Phan to find some (although not this one) security issues

- Majavah created this task. 2021-09-01 14:54:28 (UTC+0)
- Herald added projects: Universal Omega, MediaWiki (SRE). · View Herald Transcript 2021-09-01 14:54:29 (UTC+0)
- Herald added subscribers: Universal\_Omega, RhinosF1, Void, Reception123. · View Herald Transcript
- Reception123 added a comment. 2021-09-01 14:59:38 (UTC+0)



Thank you for reporting this.
- RhinosF1 added a comment. 2021-09-01 15:02:01 (UTC+0)

<https://github.com/miraheze/GlobalNewFiles/security/advisories/GHSA-57p5-hjqj-h7vg>
- RhinosF1 added a comment. 2021-09-01 15:05:23 (UTC+0)

@Majavah : there should be an option above to create a private patch, please feel free to ^
- Majavah added a comment. 2021-09-01 17:04:26 (UTC+0)

<https://github.com/miraheze/GlobalNewFiles-ghsa-57p5-hjqj-h7vg/pull/1/files>
- RhinosF1 assigned this task to Majavah. 2021-09-01 17:06:52 (UTC+0)
- RhinosF1 moved this task from Backlog to Bugs on the GlobalNewFiles board.
- RhinosF1 moved this task from Backlog to Short Term on the MediaWiki (SRE) board.
- RhinosF1 renamed this task from Stored XSS in GlobalNewFiles to Stored XSS in GlobalNewFiles (CVE-TBC). 2021-09-01 19:10:03 (UTC+0)
- RhinosF1 closed this task as Resolved.
- RhinosF1 changed the visibility from "Custom Policy" to "Public (No Login Required)".

 RhinosF1 changed the edit policy from "Custom Policy" to "All Users".

 RhinosF1 renamed this task from *Stored XSS in GlobalNewFiles (CVE-TBC)* to *Stored XSS in GlobalNewFiles (CVE-2021-39186)*. Edited - 2021-09-01 20:50:35 (UTC+0) 

*GitHub has issued CVE-2021-39186 for this Security Advisory after reviewing reviewing it for compliance with CVE rules. Once you've published your Security Advisory, we'll publish the CVE to the CVE List.*

*Thank you for making the open source ecosystem more secure by fixing and responsibly disclosing this vulnerability.*

[Log in to Comment](#)