First Last Prev Next This bug is not in your last search results.

~~Bug 1178880 - (CVE-2020-8031) VUL-0: CVE-2020-8031: obs: Stored XSS~~

Status: RESOLVED FIXED

Classification: Novell Products
Product: SUSE Security Incidents
Component: Incidents
Version: unspecified
Hardware: Other Other

Priority: P5 - None **Severity**: Normal
Target Milestone: ---
Assigned To: Security Team bot
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/271831/
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-11-17 10:46 UTC by Wolfgang Frisch
Modified: 2021-02-11 14:56 UTC (History)
CC List: 5 users (show)

See Also: ~~1178881~~

Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Wolfgang Frisch 2020-11-17 10:46:51 UTC   Description

~~~~
We received a direct report regarding a stored XSS vulnerability on the Open Build
Service front-end:

Stored XSS

# Issue Description

User can add a malicious comment to every project in OBS system. The markdown
parser used by OBS web server has a flaw which allows an attacker to inject
arbitrary attributes into html <a> tag. An attacker can make XSS attack and insert
style attribute to stretch out malicious tag to the full screen and insert
onmouseover attribute to immediately execute JavaScript code. This will result in a
situation, when an OBS user willing to check any project in OBS system will be
immediately attacked by a malicious JavaScript in a comment.

# Expected Result

Perform HTML encode of the user supplied href value.

# How to Reproduce

1. Sign up into OBS
2. Open the desired project and add the malicious comment in markdown markup with
payload e.g.

```
[-](' style="display: block; position: fixed; top: 0; left: 0; z-index: 99999;
width: 9999px; height: 9999px; font-size: 1px;" onmouseover="console.log('Stored
XSS.');var
to_delete=document.getElementsByName('hidden_id');to_delete[0].removeAttribute('style
name='hidden_id)
```

Photo 1

3. JavaScript will be executed for every project visitor almost immediately because
the tag has been stretched to the full screen and users are moving their mouse
almost all the time.
~~~~

Wolfgang Frisch 2020-11-17 16:47:08 UTC   Comment 4

~~~~
obs-server.changes:

- Update to version 2.10.4

Bugfixes
========
  Frontend
   * CVE-2020-8020: Possible stored XSS attack on comments markdown
~~~~

Johannes Segitz 2020-11-27 14:49:28 UTC   Comment 8

~~~~
Please use CVE-2020-8031 for tracking this
~~~~

Saray Cabrera Padrón 2020-12-04 12:48:44 UTC   Comment 9

We have just published a new minor release of OBS, 2.10.8, where the issue
mentioned in this ticket is fixed. CVE-2020-8031.

Marcus Meissner 2021-01-28 15:46:22 UTC Comment 10

appliance released,
hosted service was already fixed earlier

First Last Prev Next This bug is not in your last search results.

Format For Printing - XML - Clone This Bug - Top of page