

Stored XSS in various SystemGifts-related special pages (e.g. Special:SystemGiftManager, Special:ViewSystemGifts) (CVE-2021-36130)

Closed, ResolvedPublicSECURITY

Actions

Assigned To

ashley

Authored By

ashley2021-04-24 19:11:07 (UTC+0)

Tags

Security

SocialProfile (Backlog)

Vuln-XSS

SecTeam-Processed (Completed)

Social-Tools (SocialProfile)

Referenced Files

F34422610: T281043.patch

2021-04-24 20:11:23 (UTC+0)

Subscribers

Aklapper

ashley

Isarra

Icawte

Legoktm

sbassett

Description

1. As a privileged user (one with the `awardmanage` user right) go to `Special:SystemGiftManager` and create a gift that has a title like `"<script>alert('XSS')</script>`

2. Hit the button on the page to have the award created

3. Note that the XSS gets executed right away (if at least one user matches the threshold you chose)...

4. ...and as a bonus, it gets spread everywhere, or at least to the profile pages of users who got the award (though not directly - it isn't executed on `User:/User_profile:` page views, but upon clicking on the `View all` link in the user profile of a user who has more than 4 awards; e.g. **not** on `User:Foo` but definitely on `Special:ViewSystemGifts? user=Foo`)

Tangentially related bonus: the use of `$this->msg('some message key')->plain()` in `SocialProfile` in general is more than likely 100% incorrect. (I accept the full responsibility for that, my fault.)

Though they are quite similar code-wise, `UserGifts'` `Special:GiftManager` and thus the user-to-user gifting functionality does **not** seem to be affected. Likewise, the `Special:ViewGifts` and `Special:ViewGift` special pages are fine and do not execute the XSS.

Details

Project	Subject
mediawiki/extensions/SocialProfile	[SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
mediawiki/extensions/SocialProfile	[SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
mediawiki/extensions/SocialProfile	[SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
mediawiki/extensions/SocialProfile	[SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
mediawiki/extensions/SocialProfile	Add phan-taint-check plugin support to SocialProfile

Customize query in Gerrit

Related Objects

Mentions

Mentioned In

rESPR96d347eb0764: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages

rESPR44b4f89caa78: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages

rESPR58d2420c0f72: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages

rESPRf05860c593fd: Add phan-taint-check plugin support to SocialProfile

r279733: Write and send supplementary release announcement for extensions and skins with security patches (1.34.15/1.35.3/1.36.1)

r281195: Stored XSS in SportsTeams' Special:SportsTeamsManager & Special:UpdateFavoriteTeams (CVE-2021-36134)

ashley created this task. 2021-04-24 19:11:07 (UTC+0)

Restricted Application added a subscriber: Aklapper. · View Herald Transcript 2021-04-24 19:11:08 (UTC+0)

ashley claimed this task. 2021-04-24 19:13:29 (UTC+0)

ashley added projects: SocialProfile, Vuln-XSS.


ashley added a comment. 2021-04-24 20:11:23 (UTC+0)

T281043.patch23 KB

Download

Proposed patch which fixes the issues in SystemGifts spotted with the malicious award name used as an example here, adjusts `->plain()` to `->escaped()`, ensures that `LinkRenderer` is passed raw text (`->text()`) instead of escaped to avoid

double-escaping and removes parsing format from Message objects passed to `OutputPage#setPageTitle` because that method can be passed either a string or a Message object, and finally casts some things we definitely want to be ints as such (in `SpecialSystemGiftManager.php`).

 **Reedy** edited projects, added **SecTeam-Processed**; removed **Security-Team**. 2021-04-26 15:03:51 (UTC+0)

 **Legoktm** added a subscriber: **Legoktm**. 2021-04-26 15:33:55 (UTC+0)

I only reviewed the patch diff, not the rest of the code, I assume you used phan-taint-check to make sure there's no issues left?


```
<input type="hidden" name="id" value="" . ( $gift['gift_id'] ?? '' ) . "" />
```

From `SystemGiftManager`, I'd prefer if there was an `(int) cast (or intval())` just to make it obvious that `gift_id` is safe to not have explicit escaping.

```
<div class="ga-timestamp">{$gift['timestamp']}</div>
```

From `ViewSystemGift`, I think this needs escaping.

 **ashley** mentioned this in ~~**T201196: Stored XSS in SportsTeams::SpecialSportsTeamsManager & SpecialUpdateFavoriteTeams (CVE-2021-36134)**~~. 2021-04-26 22:07:42 (UTC+0)

 **ashley** added a comment. 2021-04-26 22:15:43 (UTC+0)

In ~~**T201043#7034689**~~, @**Legoktm** wrote:

I only reviewed the patch diff, not the rest of the code, I assume you used phan-taint-check to make sure there's no issues left?

Alas, `SocialProfile` does not yet to my knowledge run phan. (Just like how it doesn't support extension registration yet, or...)

From `SystemGiftManager`, I'd prefer if there was an `(int) cast (or intval())` just to make it obvious that `gift_id` is safe to not have explicit escaping.

Agreed. Implemented locally.


```
<div class="ga-timestamp">{$gift['timestamp']}</div>
```

From `ViewSystemGift`, I think this needs escaping.

As we discussed on IRC, the current (git master) implementation is indeed just a raw timestamp from the database which is barely "prettified", i.e. "2020-07-18 23:25:37"; but "23:25, 18 July 2020" is more human-friendly, so let's run that timestamp through `Language#userTimeAndDate` and thus also through `htmlspecialchars`. 🙌

Again, thanks for the review & suggestions, very helpful! 😊 Not only are we fixing obvious security issues (after ~14 years (!)) but also improving usability while it at. Yay!

 **ashley** added a project: **Social-Tools**. 2021-04-27 17:11:22 (UTC+0)

 **ashley** moved this task from **Backlog** to **SocialProfile** on the **Social-Tools** board.

 **sbassett** mentioned this in ~~**T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)**~~. 2021-04-27 18:05:01 (UTC+0)

 **sbassett** added a subscriber: **sbassett**. 2021-04-27 18:30:43 (UTC+0)

In ~~**T201043#7036127**~~, @**ashley** wrote:

In ~~**T201043#7034689**~~, @**Legoktm** wrote:

I only reviewed the patch diff, not the rest of the code, I assume you used phan-taint-check to make sure there's no issues left?

Alas, `SocialProfile` does not yet to my knowledge run phan. (Just like how it doesn't support extension registration yet, or...)

It looks like it's at least set up to use phan, as it has a [phan config](#). Having the phan-taint-check plugin available only takes a couple more steps, as noted [within the documentation](#). I've created a change set to add it here, feel free to merge if you'd like:

<https://gerrit.wikimedia.org/r/683037>

A few notes:


1. You need `php-ast` installed to run phan (and the plugin) locally, which should be as simple as `pecl install ast` in most cases.
2. `composer seccheck-fast` might emit a couple of warnings, but appears to work fine and generates a few issues, which may or may not be false positives.
3. I noticed that `composer.lock` was in `SocialProfile's .gitignore` - I think the best practice is to include this in the repo, if possible.

 **sbassett** mentioned this in **rESPRf05860c593fd: Add phan-taint-check plugin support to SocialProfile**. 2021-04-30 08:24:52 (UTC+0)

 **ashley** mentioned this in **rESPR58d2420c0f72: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages**. 2021-05-16 07:29:36 (UTC+0)

 **Legoktm** closed this task as *Resolved*. 2021-05-16 20:36:39 (UTC+0)

 **Legoktm** changed the visibility from **"Custom Policy"** to **"Public (No Login Required)"**.

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


 **gerritbot** added a comment. 2021-05-16 23:05:21 (UTC+0)

Change 692066 had a related patch set uploaded (by Southparkfan; author: Jack Phoenix):

[mediawiki/extensions/SocialProfile@REL1_35] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages

<https://gerrit.wikimedia.org/r/692066>


 **gerritbot** added a project: **Patch-For-Review**. 2021-05-16 23:05:22 (UTC+0)


 **gerritbot** added a comment. 2021-05-16 23:15:25 (UTC+0)



Change 692067 had a related patch set uploaded (by Southparkfan; author: Jack Phoenix):



[mediawiki/extensions/SocialProfile@REL1_36] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages



<https://gerrit.wikimedia.org/r/692067>

-  **gerritbot** added a comment. 2021-05-16 23:18:33 (UTC+0)

Change 692068 had a related patch set uploaded (by Southparkfan; author: Jack Phoenix):
[mediawiki/extensions/SocialProfile@REL1_31] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
<https://gerrit.wikimedia.org/r/692068>
-  **gerritbot** added a comment. 2021-05-17 01:00:30 (UTC+0)

Change 692068 **abandoned** by Jack Phoenix:
[mediawiki/extensions/SocialProfile@REL1_31] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
Reason:
Per [[mw:Social tools/MediaWiki compatibility]], the non-master release branches were never supported for social tools, especially not something as old as 1.31. We may (read: probably have to) soon transition to supporting the latest Long-Term Support (LTS) release instead of latest stable, but in any case, let's not give people the false impression that these non-master branches would be usable or recommended to be used.
<https://gerrit.wikimedia.org/r/692068>
-  **sbassett** renamed this task from *Stored XSS in various SystemGifts-related special pages (e.g. Special:SystemGiftManager, Special:ViewSystemGifts)* to *Stored XSS in various SystemGifts-related special pages (e.g. Special:SystemGiftManager, Special:ViewSystemGifts) (CVE-2021-36130)*. 2021-07-02 19:49:11 (UTC+0)
-  **gerritbot** added a comment. 2021-10-08 23:41:01 (UTC+0)

Change 692066 **merged** by jenkins-bot:
[mediawiki/extensions/SocialProfile@REL1_35] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
<https://gerrit.wikimedia.org/r/692066>
-  **Southparkfan** mentioned this in **rESPR44b4f89caa78: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages**. 2021-10-08 23:44:31 (UTC+0)
-  **gerritbot** added a comment. 2021-10-08 23:57:39 (UTC+0)

Change 692067 **merged** by jenkins-bot:
[mediawiki/extensions/SocialProfile@REL1_36] [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages
<https://gerrit.wikimedia.org/r/692067>
-  **Southparkfan** mentioned this in **rESPR96d347eb0764: [SECURITY] Fix XSS in various SystemGifts/UserGifts-related special pages**. 2021-10-08 23:59:57 (UTC+0)
-  **Maintenance_bot** removed a project: **Patch-For-Review**. 2021-10-09 00:10:18 (UTC+0)