New issue

Jump to bottom

Lack of escaping on some pages can lead to XSS exposure (CVE-2020-7106) #3191

Closed 0xfatty opened this issue on Jan 15, 2020 · 21 comments

Labels bug resolved SECURITY

0xfatty commented on Jan 15, 2020 • edited

Describe the bug
Data source input validation error leads to Stored XSS within Description after creating a device with Malicious code embedded in Description field.

To Reproduce
Steps to reproduce the behavior:

1. Navigate to Console -> Create -> New Device
2. In Description field, input script payload: `<svg/onload=alert(1)>`
3. Fill out the rest of the form as normal
4. Click Save. After the first click, there will be an error dialog saying Whitelisting is ON (yes, I turned it on this time). However, I was still able to save the "New Device" form by clicking "Save" once again.
5. After the message of "Successfully operated", click on "Data Sources" on the top right menu. XSS dialog will pop up.

You might ask me questions about CSP and the whitelisting thing in config.php:
If I turned the whitelisting feature ON? **YES**
If I fixed html.php to append CSP policy? **YES**

Screenshots

- Input fields: https://imgur.com/GcAyUkC
- Pop XSS dialog: https://imgur.com/VkMIgs2
- CSP Enabled: https://imgur.com/4A0v3jq
- XSS string was not filtered in data_sources.php: https://imgur.com/xRFHXAP

0xfatty changed the title ~~Data source~~ **Data source input validation error leads to Stored XSS within Description** on Jan 15, 2020

0xfatty changed the title ~~Data source input validation error leads to Stored XSS within Description~~ **Device Description input validation error leads to Stored XSS in data_sources.php** on Jan 15, 2020

0xfatty commented on Jan 15, 2020 Author

Remediation

- Tracing back to the code, I saw that the Description gets stored into DB. Then in data_sources.php line 1331-1332, $description takes that string (XSS) from database and then gets displayed in raw by the $header which then leads to Cross-site scripting.
- Hence, to fix this, I would suggest to run $description through htmlspecialchars() to avoid XSS payloads.

Original:

```
$description = db_fetch_cell_prepared('SELECT description FROM host WHERE id = ?', array(get_request_var('host_id')));
$header = __('Data Sources [ %s ]', $description);
```

Suggestion:

```
$description = db_fetch_cell_prepared('SELECT description FROM host WHERE id = ?', array(get_request_var('host_id')));
$description = htmlspecialchars($description, ENT_QUOTES);
$header = __('Data Sources [ %s ]', $description);
```

0xfatty changed the title ~~Device Description input validation error leads to Stored XSS in data_sources.php~~ **Vulnerability report: Device Description input validation error leads to Stored XSS in data_sources.php** on Jan 15, 2020

bmfmancini commented on Jan 15, 2020 Sponsor Contributor

Wow great catch sir!!

netniV commented on Jan 15, 2020 Member

Thanks for your ongoing efforts to improve the code Chi, appreciated. If you already have a patch, you should submit it as a pull request so we can merge it. Since this is an XSS bug, if you could do that against the 1.2.x branch and include the CHANGELOG entry too, that would be perfect.

0xfatty commented on Jan 15, 2020 Author

Hi @netniV

Thank you for your response. I am happy to do so.

cigamit commented on Jan 15, 2020 Member

Yea, I found a few more. Comitting shortly.

cigamit commented on Jan 15, 2020 Member

total files are:

- data_sources.php
- color_templates_item.php
- graphs.php
- graph_items.php
- lib/api_automation.php
- user_admin.php
- user_group_admin.php

Bummer.

cigamit changed the title ~~Vulnerability report: Device Description input validation error leads to Stored XSS in data_sources.php~~ **Vulnerability report: Lack of escaping on some pages can lead to XSS exposure** on Jan 15, 2020

cigamit added a commit that referenced this issue on Jan 15, 2020

`Resolving Issue #3191` ··· 4cbb045

cigamit commented on Jan 15, 2020 Member

Okay, just committed the fixes. That's from a pretty comprehensive audit.

cigamit commented on Jan 15, 2020 Member

@smutranchi, if you can get a CVE number for this, it would be appreciated.

cigamit added **bug** SECURITY resolved labels on Jan 15, 2020

0xfatty commented on Jan 15, 2020 Author

Hi **@cigamit** ,

Thank you for your response. I have raised a CVE request. I will put it in here once I got the number.

Sincerely,
Chi Tran

0xfatty commented on Jan 15, 2020 Author

Hi **@netniV** **@cigamit**,

A CVE was assigned to this bug as:
CVE-2020-7106.

Please let me know if you need any further information.

Best regards,
Chi Tran

netniV commented on Jan 16, 2020 Member

If you can review the code change, that would add some validation to the fix. We will use the CVE in our notifications on the next release.

cigamit added a commit that referenced this issue on Jan 16, 2020

`Update CHANGELOG for issue #3191` 3b1de37

cigamit commented on Jan 16, 2020 Member

A double review of the commit would be appreciated.

0xfatty commented on Jan 16, 2020 Author

I have just pulled new commits from 1.2.x branch and started reviewing. I will let you guys know if I found anything else.

hlef commented on Jan 18, 2020

@cigamit is can see that several lines in this diff are still missing the `__esc` :

e.g.

4cbb045 #diff-317c61020ed4b560afa7e1760f261534R1155

or

4cbb045 #diff-3398f8d2633c0b07fbd66bd7b8f75ecdR2018

Is it intentional ?

cigamit commented on Jan 18, 2020 Member

Yes, if you follow the code, those two strings are included in a subsequent __esc() further in.

0xfatty commented on Jan 19, 2020 • edited Author

Hi @cigamit ,

I noticed that when a report is created. In file lib/html_reports.php, function reports_generate_html() gets called with param $reports passed in.

Tracing back to lib/reports.php where reports_generate_html() function is declared, I observed that the report tables prints $reports['name'] in raw. (Line 707 reports.php)

Hence, if we send an XSS payload into field “Report Name”, it will still be executed when users navigate to tab Preview.

cigamit commented on Jan 19, 2020 Member

Good catch.

cigamit added a commit that referenced this issue on Jan 19, 2020

`One more update relative to #3191` … 47a000b

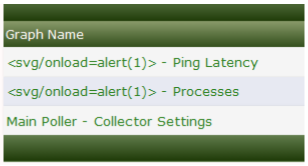
cigamit commented on Jan 19, 2020 Member

Okay, got that one caught now.

0xfatty commented on Jan 22, 2020 • edited Author

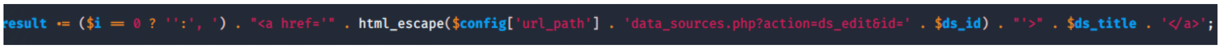
Hi @cigamit ,

I tried to trace from the Device description and got one more file that is affected.
After changing Device description to XSS payload, all graph names (title) will become `|host description| - graph feature`



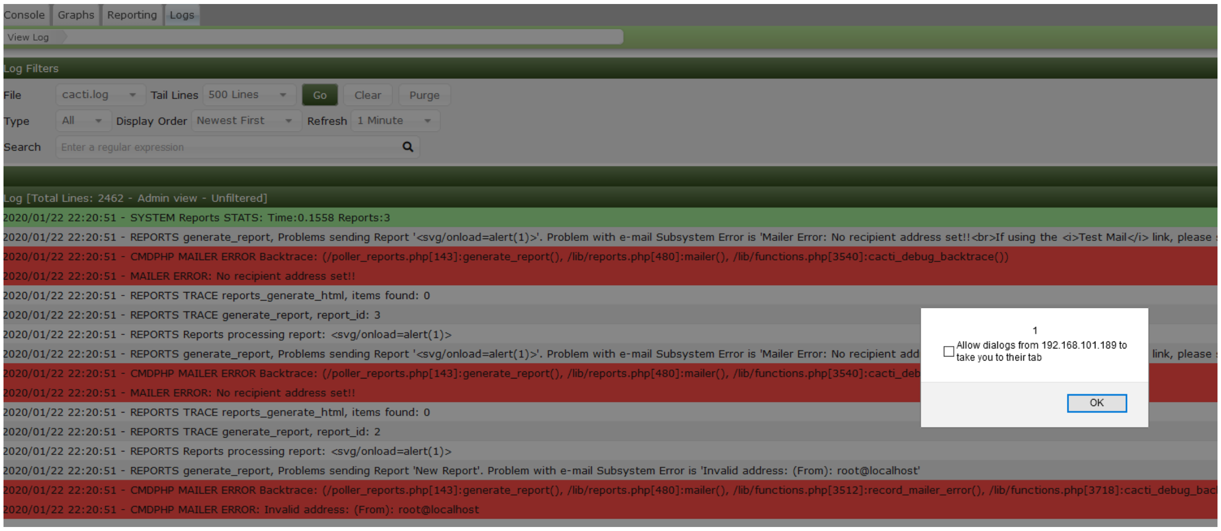
Graph Name
<svg/onload=alert(1)> - Ping Latency
<svg/onload=alert(1)> - Processes
Main Poller - Collector Settings

Then if admin turns on WEBLOG, `cli/clog_webapi.php` would be still fetching $ds_title in raw which contains XSS payload.



```
esult .= ($i == 0 ? '':', ') . "<a href='" . html_escape($config['url_path'] . 'data_sources.php?action=ds_edit&id=' . $ds_id) . "'>" . $ds_title . '</a>';
```

And pop XSS diaglog when admin navigate to Logs tab from Menu bar



File cacti.log Tail Lines 500 Lines
Type All Display Order Newest First Refresh 1 Minute
Search Enter a regular expression

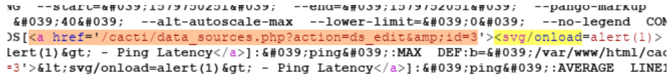
Log [Total Lines: 2462 - Admin view - Unfiltered]

```
2020/01/22 22:20:51 - SYSTEM Reports STATS: Time:0.1558 Reports:3
2020/01/22 22:20:51 - REPORTS generate_report, Problems sending Report '<svg/onload=alert(1)>'. Problem with e-mail Subsystem Error is 'Mailer Error: No recipient address set!!<br>If using the <i>Test Mail</i> link, please
2020/01/22 22:20:51 - CMDPHP MAILER ERROR Backtrace: (/poller_reports.php[143]:generate_report(), /lib/reports.php[480]:mailer(), /lib/functions.php[3540]:cacti_debug_backtrace())
2020/01/22 22:20:51 - MAILER ERROR: No recipient address set!!
2020/01/22 22:20:51 - REPORTS TRACE reports_generate_html, items found: 0
2020/01/22 22:20:51 - REPORTS TRACE generate_report, report_id: 3
2020/01/22 22:20:51 - REPORTS Reports processing report: <svg/onload=alert(1)>
2020/01/22 22:20:51 - REPORTS generate_report, Problems sending Report '<svg/onload=alert(1)>'. Problem with e-mail Subsystem Error is 'Mailer Error: No recipient add                                link, please
2020/01/22 22:20:51 - CMDPHP MAILER ERROR Backtrace: (/poller_reports.php[143]:generate_report(), /lib/reports.php[480]:mailer(), /lib/functions.php[3540]:cacti_deb
2020/01/22 22:20:51 - MAILER ERROR: No recipient address set!!
2020/01/22 22:20:51 - REPORTS TRACE reports_generate_html, items found: 0
2020/01/22 22:20:51 - REPORTS TRACE generate_report, report_id: 2
2020/01/22 22:20:51 - REPORTS Reports processing report: <svg/onload=alert(1)>
2020/01/22 22:20:51 - REPORTS generate_report, Problems sending Report 'New Report'. Problem with e-mail Subsystem Error is 'Invalid address: (From): root@localhost'
2020/01/22 22:20:51 - CMDPHP MAILER ERROR Backtrace: (/poller_reports.php[143]:generate_report(), /lib/reports.php[480]:mailer(), /lib/functions.php[3512]:record_mailer_error(), /lib/functions.php[3718]:cacti_debug_bac
2020/01/22 22:20:51 - CMDPHP MAILER ERROR: Invalid address: (From): root@localhost
```

1

☐ Allow dialogs from 192.168.101.189 to take you to their tab

OK



```
NG  --start=&#039;1579750251&#039;  --end=&#039;1579752051&#039;  --pango-markup
 &#039;40&#039;  --alt-autoscale-max  --lower-limit=&#039;0&#039;  --no-legend  COM
DS[<a href='/cacti/data_sources.php?action=ds_edit&amp;id=3'><svg/onload=alert(1)>
lert(1)&gt; - Ping Latency</a>]:&#039;ping&#039;:MAX  DEF:b=&#039;/var/www/html/cac
=3'>&lt;svg/onload=alert(1)&gt; - Ping Latency</a>]:&#039;ping&#039;:AVERAGE  LINE1
```

0xfatty commented on Jan 22, 2020 • edited ▾ Author

I have just also made a change to 1.2.x branch on clog_webapi.php file.

0xfatty pushed a commit to 0xfatty/cacti that referenced this issue on Jan 22, 2020

`update relative to issue Cacti#3191` e383b1f

0xfatty mentioned this issue on Jan 22, 2020

Patch 2 #3212

Closed

0xfatty pushed a commit to 0xfatty/cacti that referenced this issue on Jan 22, 2020

`update relative to issue Cacti#3191` 39e98e3

netniV commented on Jan 23, 2020 Member

Thanks again Chi, I'll take a look and see about submitting it.

netniV pushed a commit that referenced this issue on Jan 23, 2020

`update relative to issue #3191 (#3213)` b1c70e1

TheWitness closed this as completed on Jan 23, 2020

netniV changed the title ~~Vulnerability report: Lack of escaping on some pages can lead to XSS exposure~~ Lack of escaping on some pages can lead to XSS exposure (CVE-2020-7106) on Feb 9, 2020

ddb4github mentioned this issue on Feb 11, 2020

Should merge CVE-2020-7106 solution to syslog plugin Cacti/plugin_syslog#109

Closed

ddb4github mentioned this issue on Apr 16, 2020

Lack of escaping of color items can lead to XSS exposure (CVE-2020-7106) #3467

Closed

TheWitness added a commit that referenced this issue on Apr 16, 2020

`Fixing Issue #3467 …` 41a0cad

This was referenced on Apr 17, 2020

Fixed: Update more lines to resolve XSS exposure (CVE-2020-7106) Cacti/plugin_syslog#122

Merged

Fixed: Update more lines to resolve XSS exposure (CVE-2020-7106) Cacti/plugin_thold#422

Merged

github-actions bot locked and limited conversation to collaborators on Jun 30, 2020

Assignees

No one assigned

Labels

bug resolved SECURITY

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants