New issue

Jump to bottom

Lack of escaping on some pages can lead to XSS exposure #3549

Closed ddb4github opened this issue on May 10, 2020 · 27 comments

Labels bug resolved SECURITY

Milestone 1.2.13

ddb4github commented on May 10, 2020 • edited Contributor

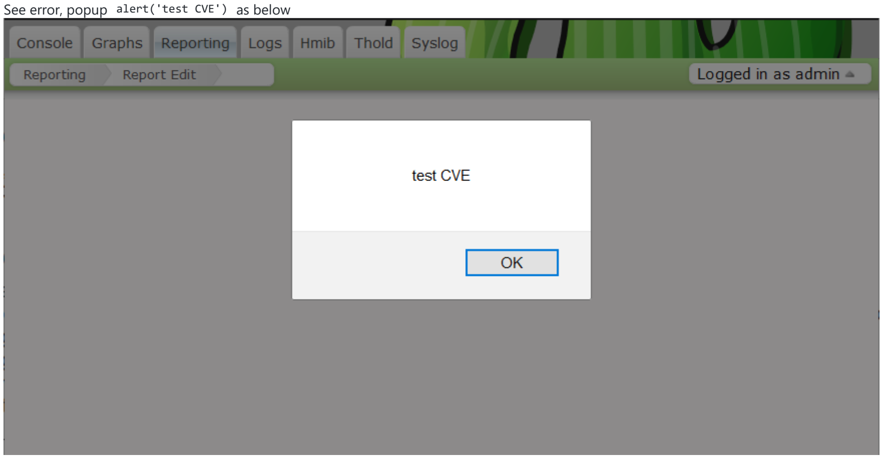
Describe the bug

Several XSS Vulnerabilities during XSS testing

To Reproduce

Case#1

1. Go to 'Reporting(reports_admin.php)'
2. Create/Modify a report
3. Add a 'Text' item with Fixed Text `<script>alert('test CVE');</script>`
4. Click save, and then return to Item list
5. See error, popup `alert('test CVE')` as below

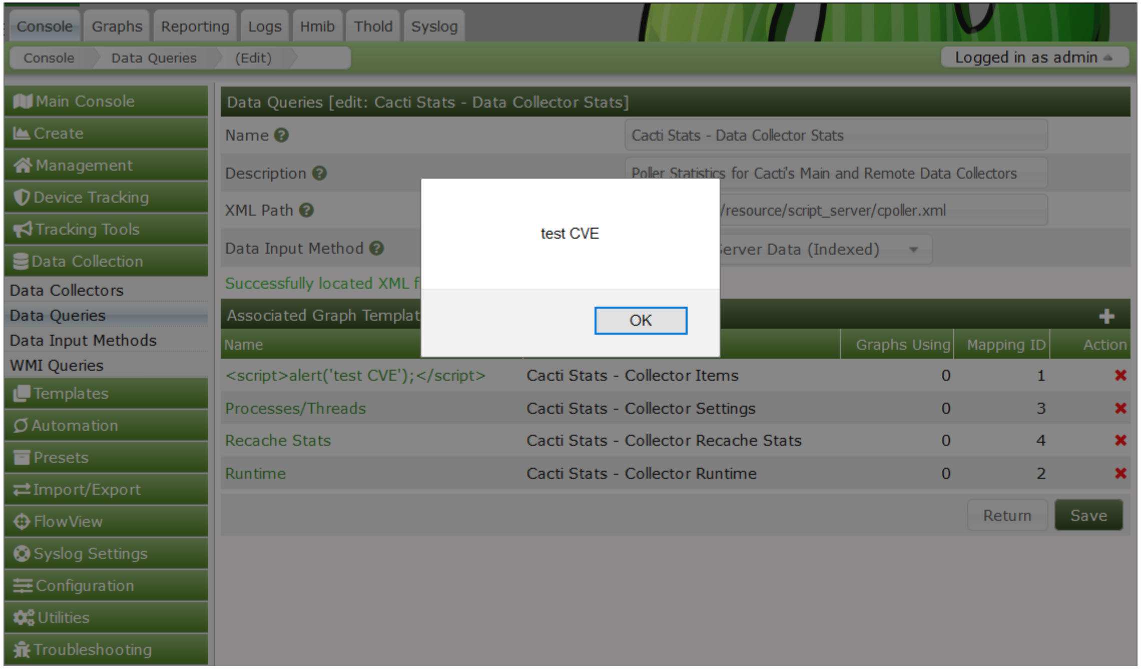


6. Click 'Preview' tab
7. See error again.

Case#2

1. Go to 'Console -> Data Collection -> Data Queries'
2. Select a data query, and click name to edit it
3. Click `name` of one of `Associated Graph Templates`
4. Modify name to `<script>alert('test CVE');</script>`
5. Click Save button, then click Return button
6. Click `x` icon of row right for the modified one

7. See error, popup `alert('test CVE')` as below



Data Queries [edit: Cacti Stats - Data Collector Stats]

Name: Cacti Stats - Data Collector Stats

Description: Poller Statistics for Cacti's Main and Remote Data Collectors

XML Path: /resource/script_server/cpoller.xml

Data Input Method: erver Data (Indexed)

Successfully located XML f

test CVE

Associated Graph Templat

Name		Graphs Using	Mapping ID	Action
<script>alert('test CVE');</script>	Cacti Stats - Collector Items	0	1	✖
Processes/Threads	Cacti Stats - Collector Settings	0	3	✖
Recache Stats	Cacti Stats - Collector Recache Stats	0	4	✖
Runtime	Cacti Stats - Collector Runtime	0	2	✖

Case#3

data_input.php, delete,click a output/input field with <script>alert('test CVE');</script>

Case#4

graph_templates.php add graph items with a color named <script>alert('test CVE');</script>

Case#5

1. Go to 'Console -> Management`
2. Add a XSS Site with name `<script>alert('SiteCore');</script>`
3. Add a XSS Device with name: `<script>alert('hostname');</script>` , description: `<script>alert('hostdesc');</script>`
4. Access any 'Console -> Management -> Trees`
5. Click any one of tree name
6. See error, popup twice `alert('SiteCore')` , `alert('hostdesc')` , `alert('hostname')` .

Case#6

1. Go to 'Console -> Management -> Trees`
2. Crate a tree with name `<script>alert('tree');</script>`
3. Access 'Console -> Management -> Graphs`
4. Select any one of graph
5. Select Action `Place on a Tree <script>alert('tree');</script>`
6. Click Go
7. See error, popup `alert('tree')`

Case#7

1. Edit a graph template, fill name with `<script>alert('gtemplatename');</script>`
2. Edit or create a report with name `<script>alert('rptname');</script>`
3. Access Graphs --> List/Tree/Preview mode
4. See error, tree/preview will popup `alert('gtemplatename')` only. And list mode will popup a extra `alert('rptname')`

Case#8

1. Edit or create a graph template, fill name with `<script>alert('gtemplatename');</script>`
2. Associate above graph template to a device
3. Edit above device
4. Click hyperlink `Create Graphs for this Device`
5. Select above graph template in list
6. Click "Create" button
7. See error

Desktop (please complete the following information)

- OS: Windows 10
- Browser: Firefox
- Version: 68.8 ESR

ddb4github added bug unverified labels on May 10, 2020

TheWitness commented on May 11, 2020 Member

Jing, can you request a CVE#?

TheWitness commented on May 11, 2020 Member

Case #2 is not repeatable in 1.2.12.

TheWitness commented on May 11, 2020 Member

Okay, was able to verify issue #2, but issue #5 and #6 you need to provide additional details.

TheWitness added a commit that referenced this issue on May 11, 2020

`Fixing Issue #3549` … `8d5fbc4`

TheWitness added resolved and removed unverified labels on May 11, 2020

TheWitness added this to the **1.2.13** milestone on May 11, 2020

ddb4github commented on May 12, 2020 Contributor Author

> Okay, was able to verify issue #2, but issue #5 and #6 you need to provide additional details.

Updated Case#5 and Case#6 for detail steps

ddb4github commented on May 12, 2020 Contributor Author

> Jing, can you request a CVE#?

Just request, to be reviewed

netniV commented on May 12, 2020 Member

Thanks **@ddb4github**! When I first started seeing these CVE's, it was upsetting as no one likes holes in their code, but at the same time we are very grateful that people are using the product and testing it thoroughly to help find these things 👍

Keep up the good work

TheWitness added a commit that referenced this issue on May 13, 2020

`Additional Fix to #3549` … `74c011b`

TheWitness added a commit that referenced this issue on May 13, 2020

`Additional Fixes for #3549` … `5e4c77e`

TheWitness commented on May 13, 2020 Member

Okay, all resolved. Thanks Jing.

ddb4github commented on May 19, 2020 Contributor Author

append Case7,8 to Issue Desc area

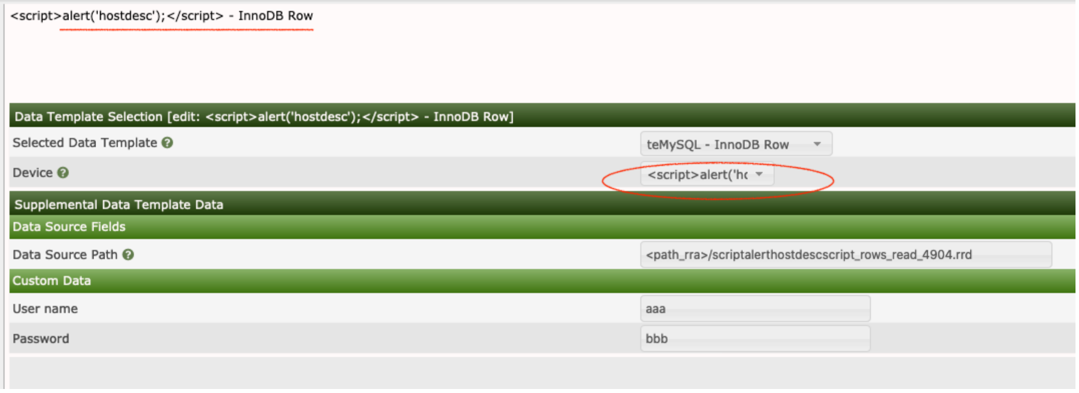
yingbaiibm commented on May 20, 2020

Append more cases

Case #9 data_sources.php page with popup exist

1. Add a device with name <script>alert(1);</script>
2. Create graph for the device

3. Go to Data Sources page, click the data source with name <script>alert(1);</script>, pop up exist

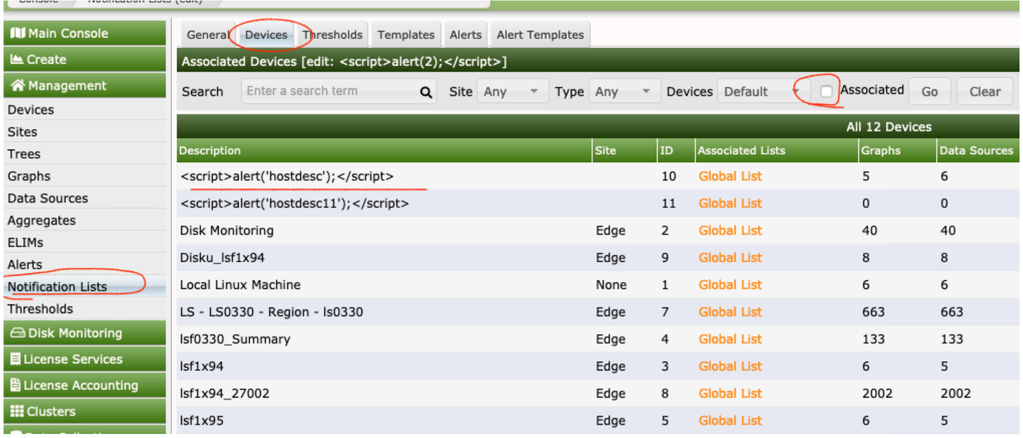


<script>alert('hostdesc');</script> - InnoDB Row

Data Template Selection [edit: <script>alert('hostdesc');</script> - InnoDB Row]	
Selected Data Template	teMySQL - InnoDB Row
Device	<script>alert('hc
Supplemental Data Template Data	
Data Source Fields	
Data Source Path	<path_rra>/scriptalerthostdescscript_rows_read_4904.rrd
Custom Data	
User name	aaa
Password	bbb

Case #10 notify_lists.php with popup exist

1. add a notification
2. go to device page, popup exist due to there is device name as <script>alert(1);</script>



Associated Devices [edit: <script>alert(2);</script>]

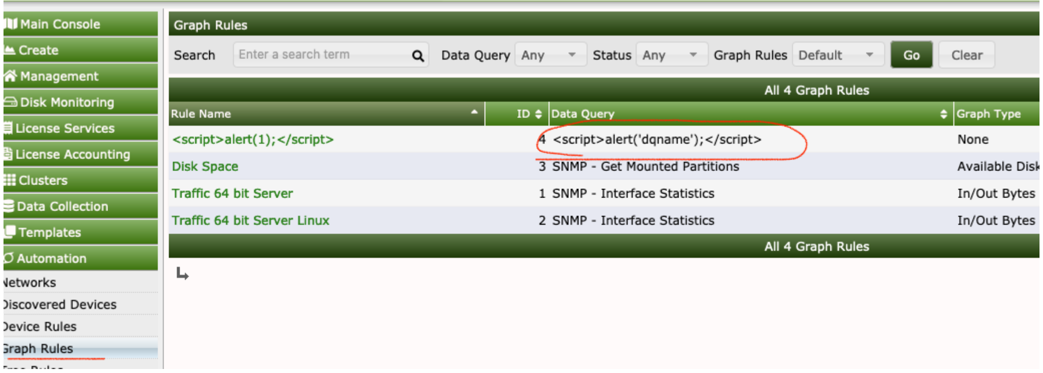
Search: Enter a search term | Site: Any | Type: Any | Devices: Default | ☐ Associated

All 12 Devices

Description	Site	ID	Associated Lists	Graphs	Data Sources
<script>alert('hostdesc');</script>		10	Global List	5	6
<script>alert('hostdesc11');</script>		11	Global List	0	0
Disk Monitoring	Edge	2	Global List	40	40
Disku_lsf1x94	Edge	9	Global List	8	8
Local Linux Machine	None	1	Global List	6	6
LS - LS0330 - Region - ls0330	Edge	7	Global List	663	663
lsf0330_Summary	Edge	4	Global List	133	133
lsf1x94	Edge	3	Global List	6	5
lsf1x94_27002	Edge	8	Global List	2002	2002
lsf1x95	Edge	5	Global List	6	5

Case #11 automation_graph_rules.php popup exist on page

1. Go to automation - Graph Rules page
2. Add a rule with name and data query as <script>alert(1);</script> and save it.
3. Click Graph Rules page again, popup exist.



Graph Rules

Search: Enter a search term | Data Query: Any | Status: Any | Graph Rules: Default

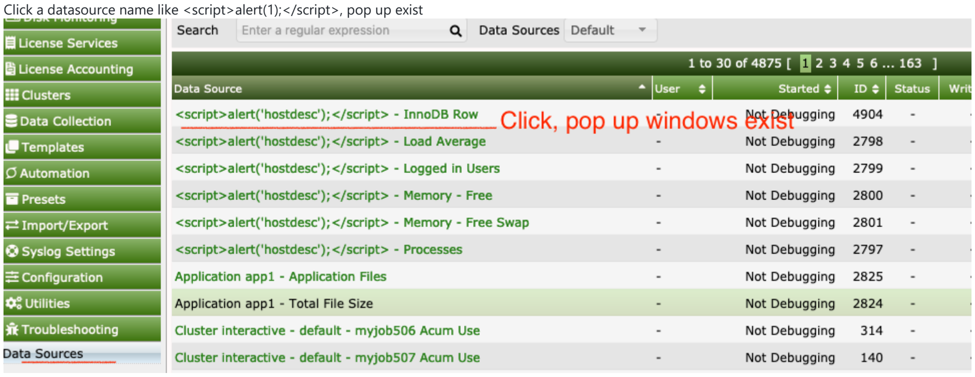
All 4 Graph Rules

Rule Name	ID	Data Query	Graph Type
<script>alert(1);</script>	4	<script>alert('dqname');</script>	None
Disk Space	3	SNMP - Get Mounted Partitions	Available Disk
Traffic 64 bit Server	1	SNMP - Interface Statistics	In/Out Bytes
Traffic 64 bit Server Linux	2	SNMP - Interface Statistics	In/Out Bytes

All 4 Graph Rules

Case #12 data_debug.php, edit a datasource with script has popup exist

1. Go to TroubleShooting - Data Sources page
2. Click a datasource name like <script>alert(1);</script>, pop up exist



Search: Enter a regular expression | Data Sources: Default

1 to 30 of 4875 [1 2 3 4 5 6 ... 163]

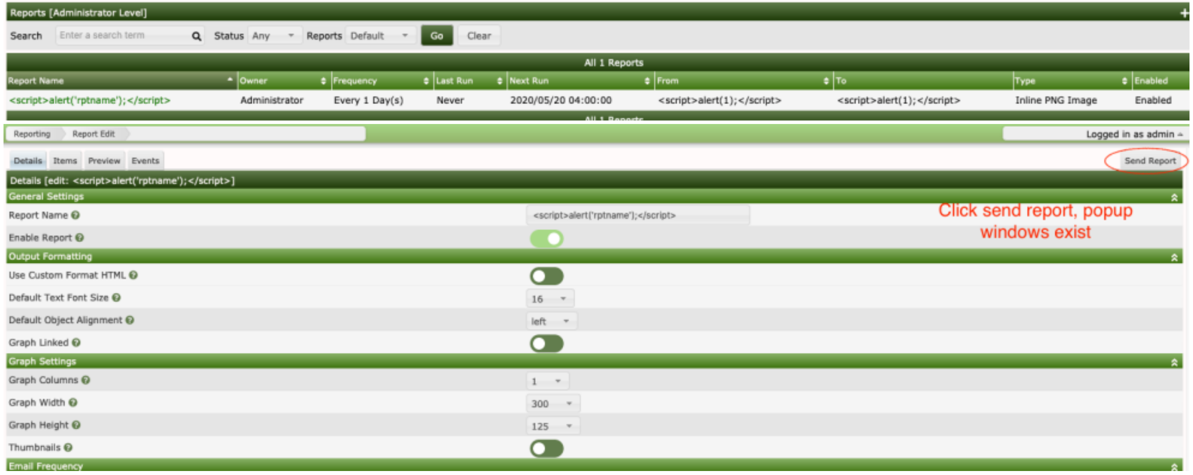
Data Source	User	Started	ID	Status	Writ
<script>alert('hostdesc');</script> - InnoDB Row	-	Not Debugging	4904	-	
<script>alert('hostdesc');</script> - Load Average	-	Not Debugging	2798	-	
<script>alert('hostdesc');</script> - Logged in Users	-	Not Debugging	2799	-	
<script>alert('hostdesc');</script> - Memory - Free	-	Not Debugging	2800	-	
<script>alert('hostdesc');</script> - Memory - Free Swap	-	Not Debugging	2801	-	
<script>alert('hostdesc');</script> - Processes	-	Not Debugging	2797	-	
Application app1 - Application Files	-	Not Debugging	2825	-	
Application app1 - Total File Size	-	Not Debugging	2824	-	
Cluster interactive - default - myjob506 Acum Use	-	Not Debugging	314	-	
Cluster interactive - default - myjob507 Acum Use	-	Not Debugging	140	-	

Click, pop up windows exist

yingbaiibm commented on May 20, 2020

Case #13 reports_admin.php, add an item with script, click send now, pop up exist

1. add report name like <script>alert(1);</script>
2. Click the report
3. Click send report, popup windows exist



Report Name	Owner	Frequency	Last Run	Next Run	From	To	Type	Enabled
<script>alert('rptname');</script>	Administrator	Every 1 Day(s)	Never	2020/05/20 04:00:00	<script>alert(1);</script>	<script>alert(1);</script>	Inline PNG Image	Enabled

Details [edit: <script>alert('rptname');</script>]

General Settings

Report Name	<script>alert('rptname');</script>
Enable Report	

Output Formatting

Use Custom Format HTML	
Default Text Font Size	16
Default Object Alignment	left
Graph Linked	

Graph Settings

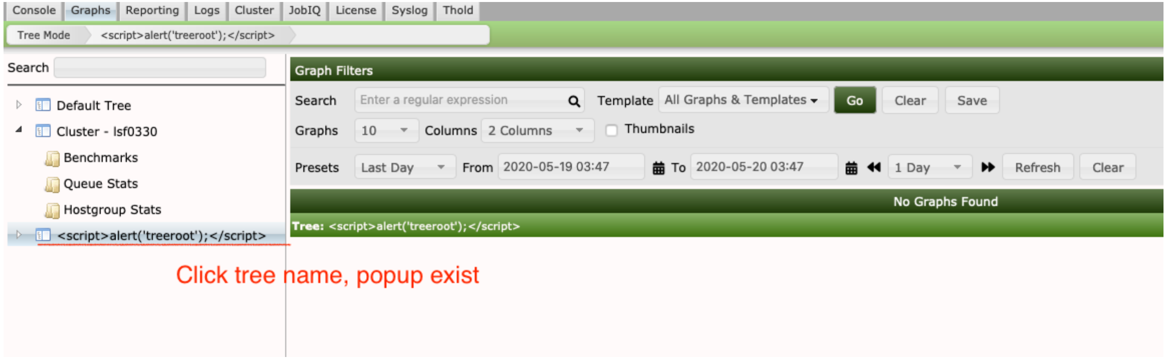
Graph Columns	1
Graph Width	300
Graph Height	125
Thumbnails	

Email Frequency

Click send report, popup windows exist

Case #14 click a tree named with script has popup

1. Create a tree name like <script>alert(1);</script>
2. publish the tree
3. Go to graph page, click the tree name, popup exist

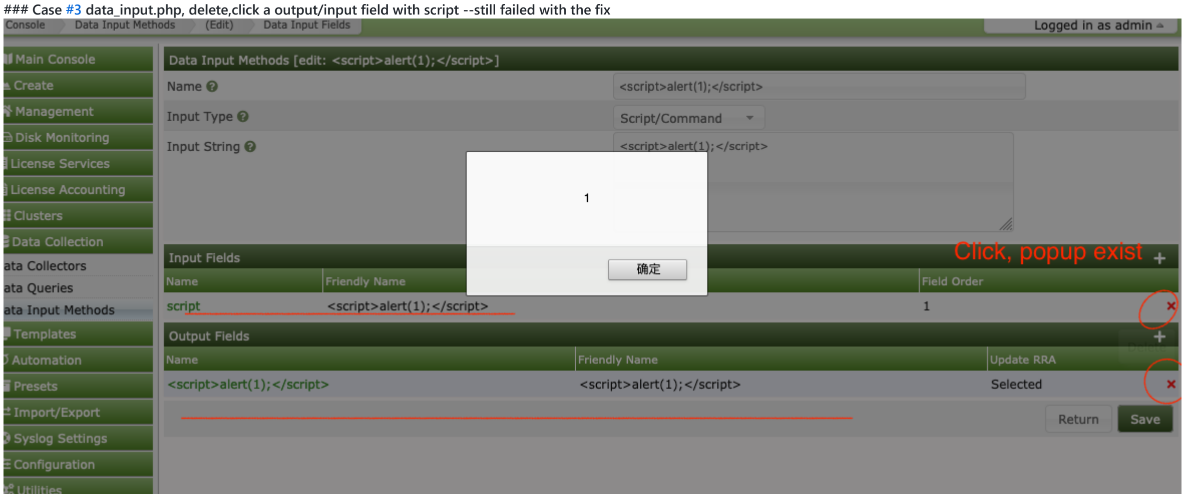


No Graphs Found

Tree: <script>alert('treeroot');</script>

Click tree name, popup exist

Case #3 data_input.php, delete,click a output/input field with script --still failed with the fix



Data Input Methods [edit: <script>alert(1);</script>]

Name	<script>alert(1);</script>
Input Type	Script/Command
Input String	<script>alert(1);</script>

Input Fields

Name	Friendly Name	Field Order
script	<script>alert(1);</script>	1

Output Fields

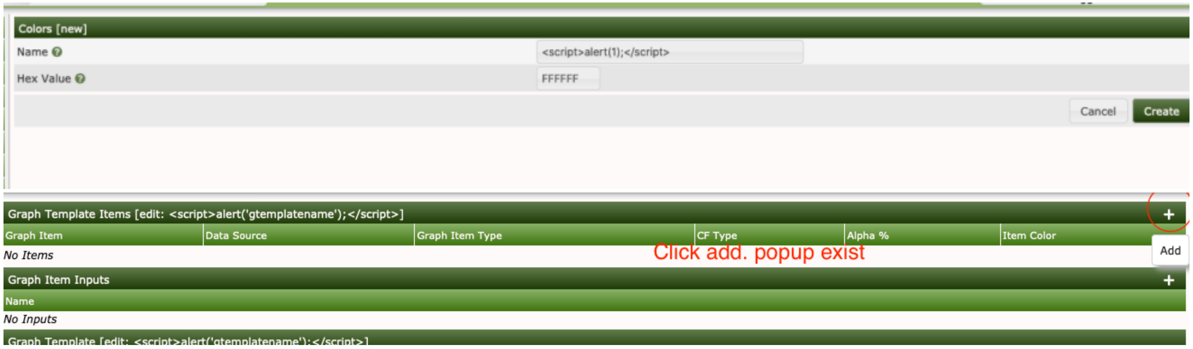
Name	Friendly Name	Update RRA
<script>alert(1);</script>	<script>alert(1);</script>	Selected

Click, popup exist

Case #4 graph_templates.php add graph items with a color named --failed with the fix

1. Go to Present - Colors
2. Add a color named like <script>alert(1);</script>
3. Go to Template -Graph page
4. Add a graph template

5. Click add graph item, popup exist



Colors [new]

Name	<script>alert(1);</script>
Hex Value	FFFFFF

Graph Template Items [edit: <script>alert('gtemplatename');</script>]

Graph Item	Data Source	Graph Item Type	CF Type	Alpha %	Item Color

No Items

Click add. popup exist

Graph Item Inputs

Name

No Inputs

Graph Template [edit: <script>alert('gtemplatename');</script>]

netniV commented on May 20, 2020 Member

Case #9 seems to be directly related to using drop_callback, as when you change the field to a textbox, the XSS doesn't exist.

Case #10 is specific to Thold so should be opened against that repo.

Case #11 is due to the Data Query drop down not being escaped.

Case #12 is due to the title not being escaped on the *Were we able to convert the title?* line.

Case #13 is due to the title not being escaped in the success/fail messages.

Case #14 is something i was unable to reproduce.

netniV added a commit that referenced this issue on May 20, 2020

`Further fixes for #3549` 798f499

netniV commented on May 20, 2020 • edited Member

I have sorted 11 through 13, the rest are unresolved or unconfirmed.

netniV added SECURITY and removed resolved labels on May 20, 2020

TheWitness added a commit that referenced this issue on May 20, 2020

`More fixing for issue #3549` … dc35a79

TheWitness commented on May 20, 2020 Member

I've fixed a few more of these. I guess we need to hit a reset button. **@yingbaiibm**, can you summarize what is still outstanding?

yingbaiibm commented on May 21, 2020

@TheWitness ok, I will check and summarize the status after we merge the new fix.

yingbaiibm commented on May 29, 2020

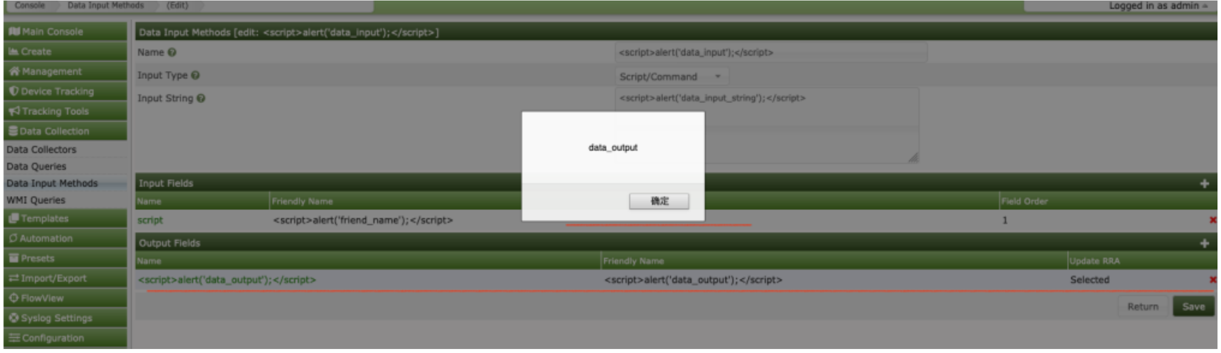
@TheWitness Test using latest cacti code, make a summray like below.
passed retest 10 cases, failed 4 cases, added 5 new cases. see details like below

yingbaiibm commented on May 29, 2020

passed case: 1, 2, 5, 6, 8, 10, 11, 12, 13, 14

Failed case 3, 4, 7, 9

Case3: click/delete a data output field has popup exist



Data Input Methods [edit: <script>alert('data_input');</script>]

Name	<script>alert('data_input');</script>
Input Type	Script/Command
Input String	<script>alert('data_input_string');</script>

data_output

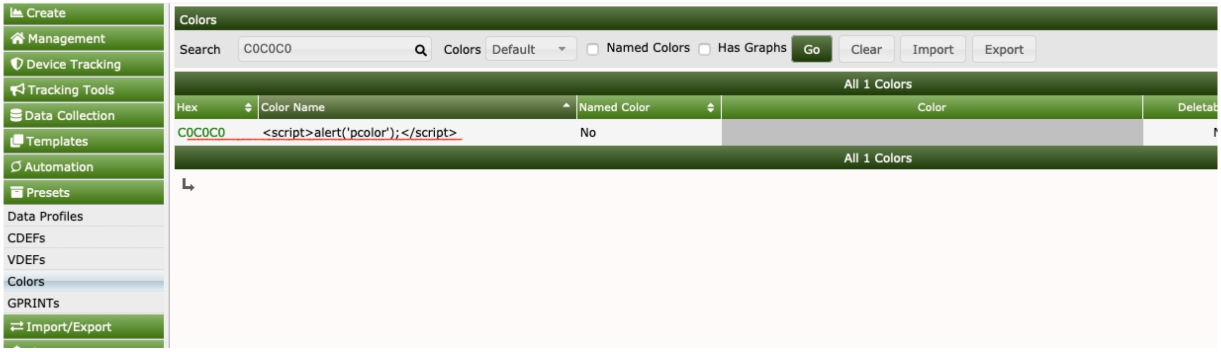
Input Fields

Name	Friendly Name	Field Order
script	<script>alert('friend_name');</script>	1

Output Fields

Name	Friendly Name	Update RRA
<script>alert('data_output');</script>	<script>alert('data_output');</script>	Selected

Case4: graph_templates.php add graph items with a color named
- go to present-color, add a color named with <script>alert('pcolor');</script>
- go to template graph, add a graph, add a graph item, popup exist

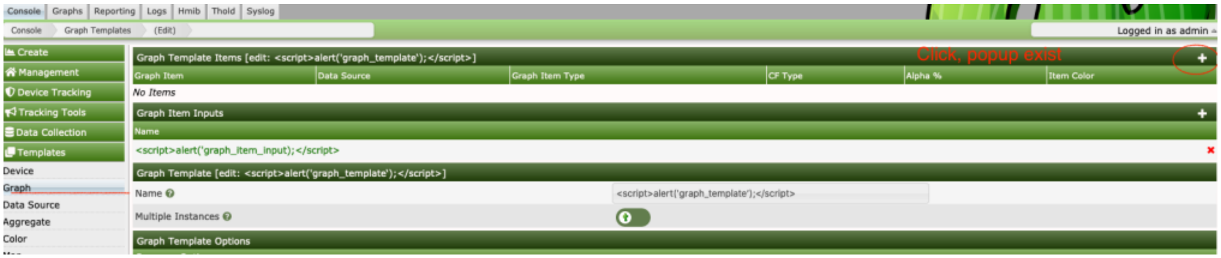


Search C0C0C0

All 1 Colors

Hex	Color Name	Named Color	Color	Deletab
C0C0C0	<script>alert('pcolor');</script>	No		N

All 1 Colors



Graph Template Items [edit: <script>alert('graph_template');</script>]

Graph Item	Data Source	Graph Item Type	CF Type	Alpha %	Item Color
No Items					

Graph Item Inputs

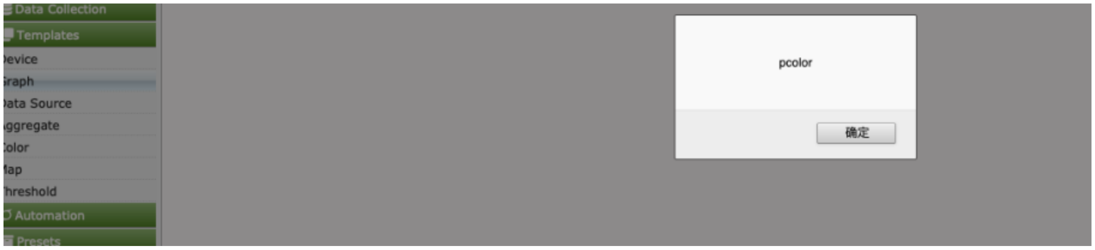
Name
<script>alert('graph_item_input);</script>

Graph Template [edit: <script>alert('graph_template');</script>]

Name <script>alert('graph_template');</script>

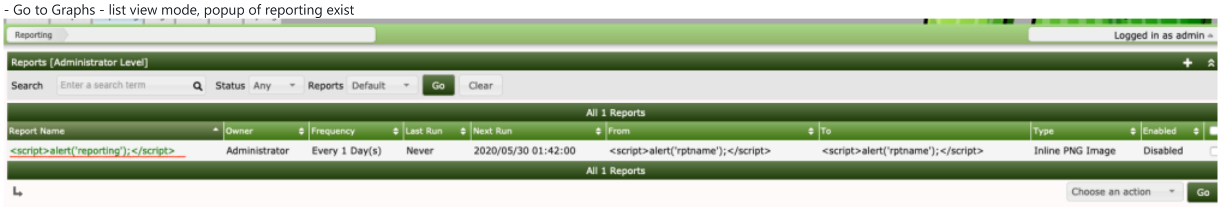
Multiple Instances

Graph Template Options



pcolor

case7 go to graphs - list view mode, popup exist for reporting with name <script>alert('xxx');</script>
- Go to Reporting page, add a report name with <script>alert('reporting');</script>
- Go to Graphs - list view mode, popup of reporting exist

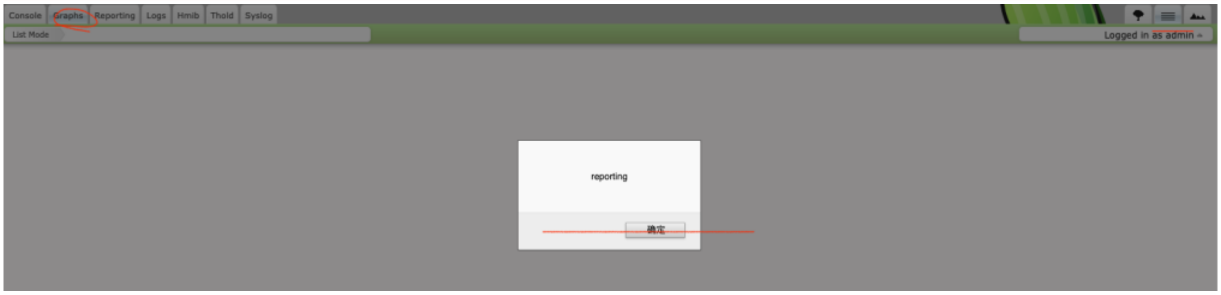


Reports [Administrator Level]

All 1 Reports

Report Name	Owner	Frequency	Last Run	Next Run	From	To	Type	Enabled
<script>alert('reporting');</script>	Administrator	Every 1 Day(s)	Never	2020/05/30 01:42:00	<script>alert('rptname');</script>	<script>alert('rptname');</script>	Inline PNG Image	Disabled

All 1 Reports

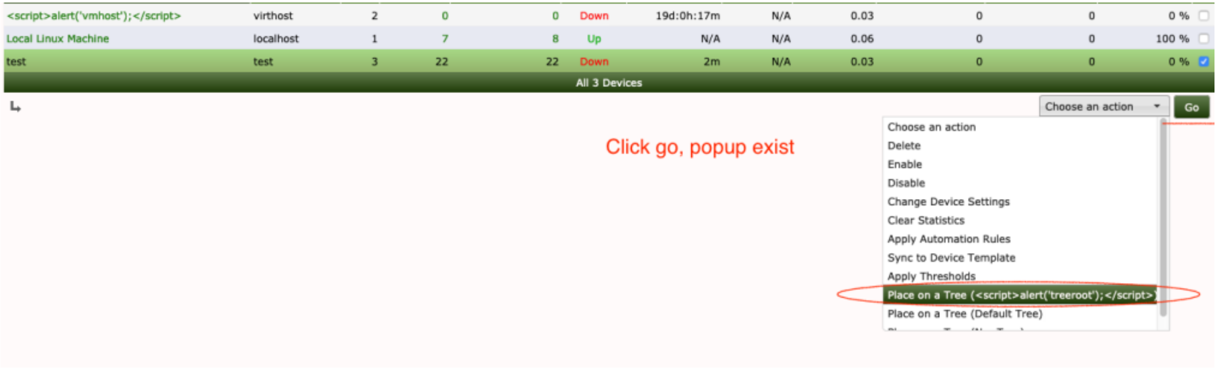


reporting

Case9 data_sources.php page with popup exist

New founded issue

Case#15 place device on a tree named with <script>alert('tree');</script> has popup exist



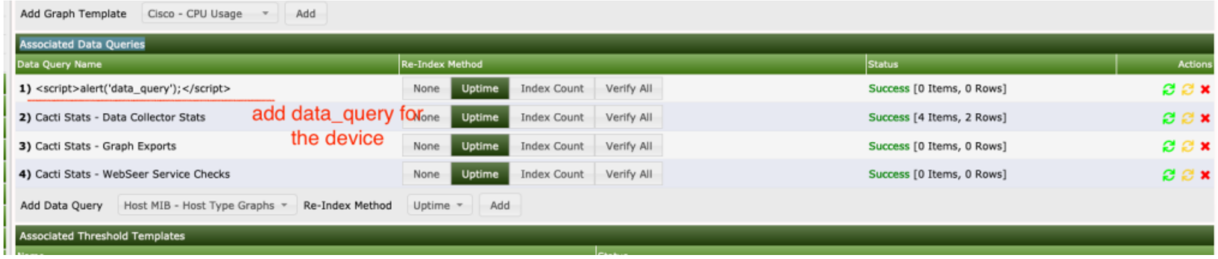
<script>alert('vmhost');</script>	virthost	2	0	0	Down	19d:0h:17m	N/A	0.03	0	0	0 %	□
Local Linux Machine	localhost	1	7	8	Up	N/A	N/A	0.06	0	0	100 %	□
test	test	3	22	22	Down	2m	N/A	0.03	0	0	0 %	☑

All 3 Devices

Click go, popup exist

Case#16 create graph for a device has popup exist due to data query with script

- create a data query with name <script>alert('data_query');</script>
- Go to device page, add the data_query to the device
- Click create graphs for this device, popup exist

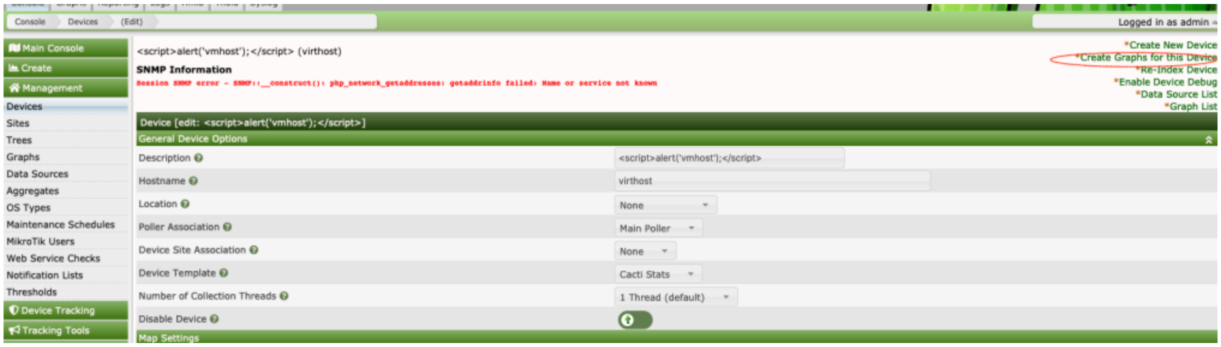


Associated Data Queries

Data Query Name	Re-Index Method	Status	Actions
1) <script>alert('data_query');</script>	None Uptime Index Count Verify All	Success [0 Items, 0 Rows]	
2) Cacti Stats - Data Collector Stats	None Uptime Index Count Verify All	Success [4 Items, 2 Rows]	
3) Cacti Stats - Graph Exports	None Uptime Index Count Verify All	Success [0 Items, 0 Rows]	
4) Cacti Stats - WebSeer Service Checks	None Uptime Index Count Verify All	Success [0 Items, 0 Rows]	

add data_query for the device

Associated Threshold Templates



<script>alert('vmhost');</script> (virthost)

SNMP Information

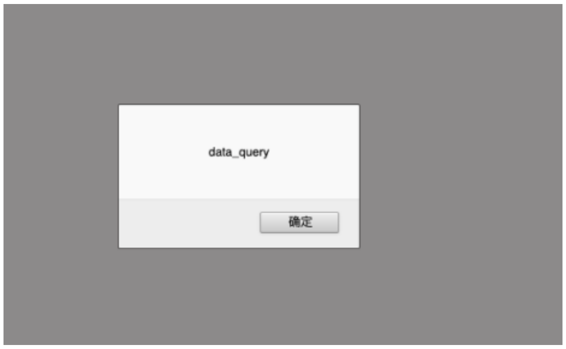
```
Session SNMP error - SNMP::__construct(): php_network_getaddresses: getaddrinfo failed: Name or service not known
```

Device [edit: <script>alert('vmhost');</script>]

General Device Options

Description: <script>alert('vmhost');</script>
Hostname: virthost
Location: None
Poller Association: Main Poller
Device Site Association: None
Device Template: Cacti Stats
Number of Collection Threads: 1 Thread (default)
Disable Device

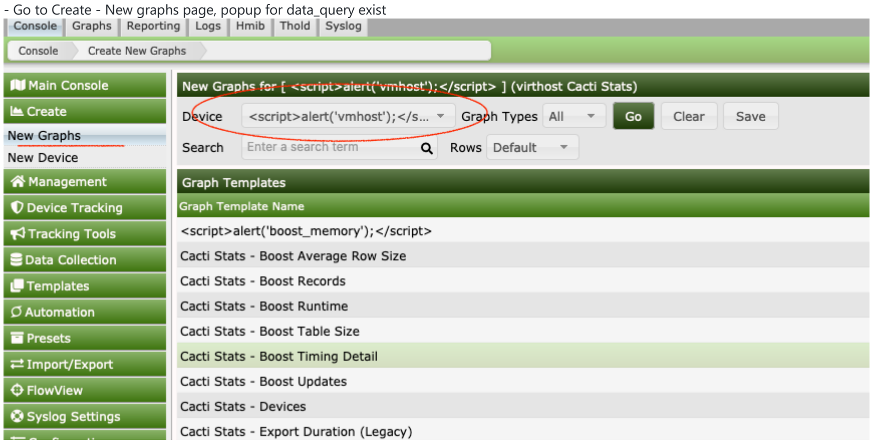
Map Settings



data_query

Case#17 go to create graph page, popup exist

- create a data query with name <script>alert('data_query');</script>
- Go to device page, add the data_query to the device
- Go to Create - New graphs page, popup for data_query exist



New Graphs for [<script>alert('vmhost');</script>] (virthost Cacti Stats)

Device <script>alert('vmhost');</s... Graph Types All

Search Enter a search term Rows Default

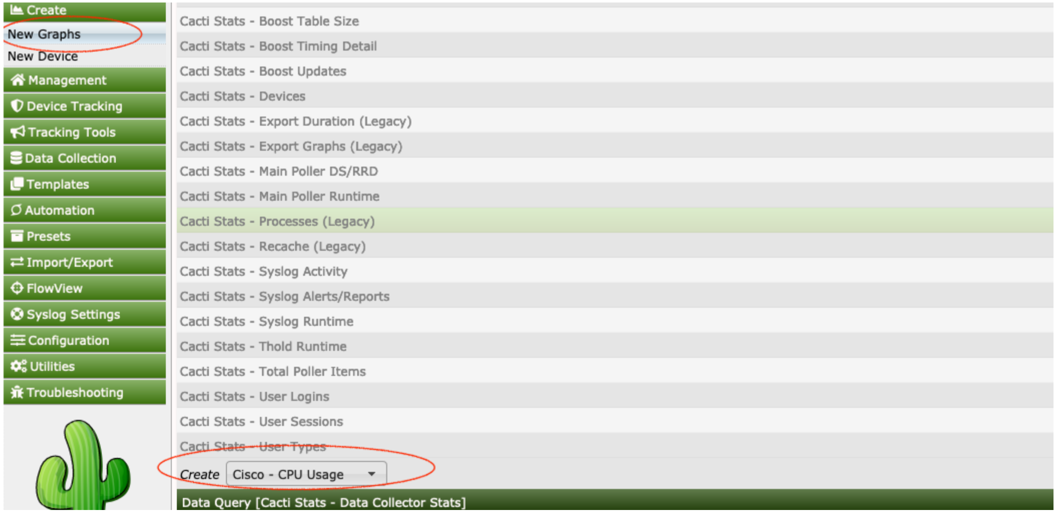
Graph Templates

Graph Template Name

<script>alert('boost_memory');</script>
Cacti Stats - Boost Average Row Size
Cacti Stats - Boost Records
Cacti Stats - Boost Runtime
Cacti Stats - Boost Table Size
Cacti Stats - Boost Timing Detail
Cacti Stats - Boost Updates
Cacti Stats - Devices
Cacti Stats - Export Duration (Legacy)

Case#18 create graph for a device has popup exist for color with script

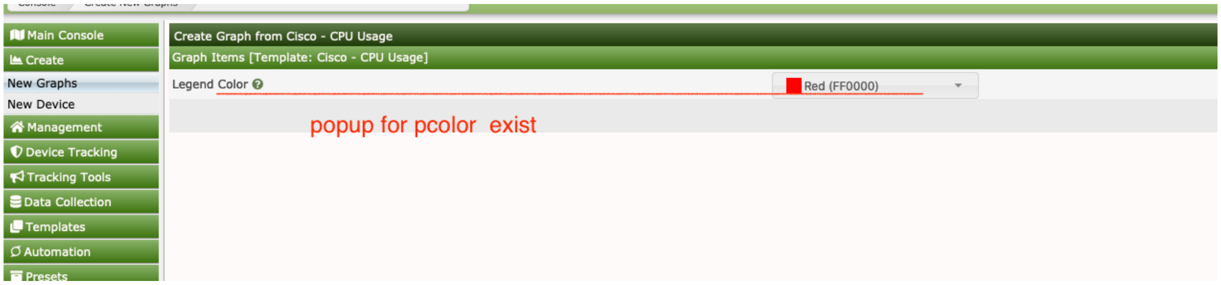
- go to present-color, add a color named with <script>alert('pcolor');</script>
- Create a graph for device, choose Cisco- CPU Usage Graph template
- Click create, popup for pcolor exist



Cacti Stats - Boost Table Size
Cacti Stats - Boost Timing Detail
Cacti Stats - Boost Updates
Cacti Stats - Devices
Cacti Stats - Export Duration (Legacy)
Cacti Stats - Export Graphs (Legacy)
Cacti Stats - Main Poller DS/RRD
Cacti Stats - Main Poller Runtime
Cacti Stats - Processes (Legacy)
Cacti Stats - Recache (Legacy)
Cacti Stats - Syslog Activity
Cacti Stats - Syslog Alerts/Reports
Cacti Stats - Syslog Runtime
Cacti Stats - Thold Runtime
Cacti Stats - Total Poller Items
Cacti Stats - User Logins
Cacti Stats - User Sessions
Cacti Stats - User Types

Create Cisco - CPU Usage

Data Query [Cacti Stats - Data Collector Stats]



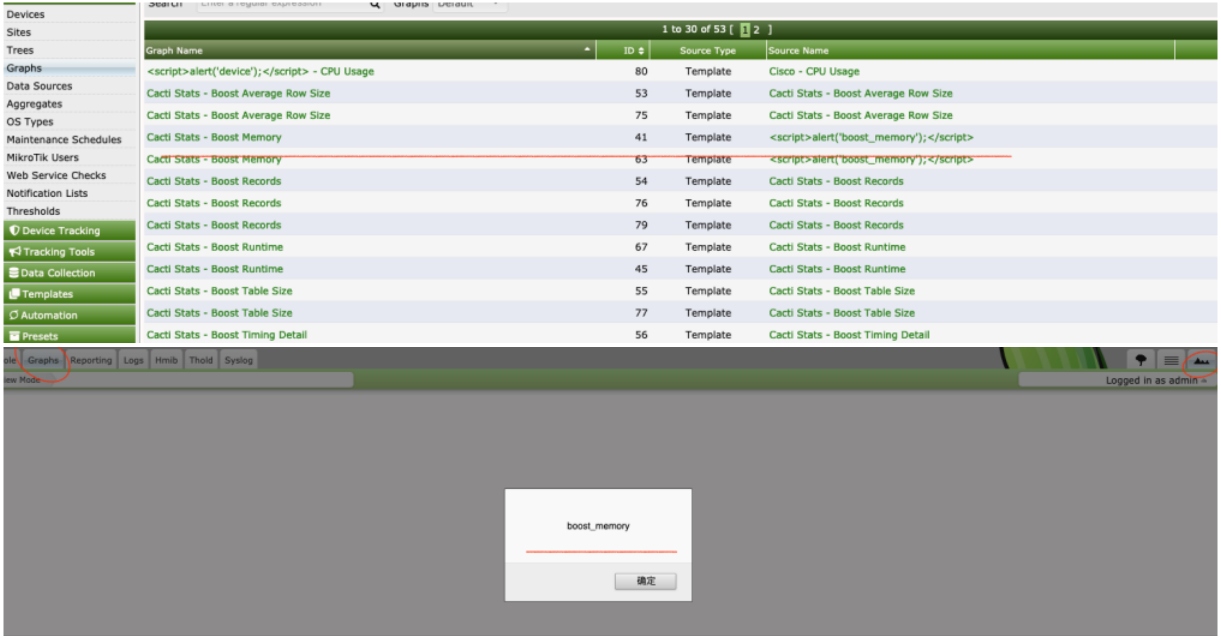
Create Graph from Cisco - CPU Usage

Graph Items [Template: Cisco - CPU Usage]

Legend Color 🟥 Red (FF0000)

popup for pcolor exist

Case#19 go to graphs - preview mode has popup for graph name with script



1 to 30 of 53 [1 2]

Graph Name	ID	Source Type	Source Name
<script>alert('device');</script> - CPU Usage	80	Template	Cisco - CPU Usage
Cacti Stats - Boost Average Row Size	53	Template	Cacti Stats - Boost Average Row Size
Cacti Stats - Boost Average Row Size	75	Template	Cacti Stats - Boost Average Row Size
Cacti Stats - Boost Memory	41	Template	<script>alert('boost_memory');</script>
Cacti Stats - Boost Memory	63	Template	<script>alert('boost_memory');</script>
Cacti Stats - Boost Records	54	Template	Cacti Stats - Boost Records
Cacti Stats - Boost Records	76	Template	Cacti Stats - Boost Records
Cacti Stats - Boost Records	79	Template	Cacti Stats - Boost Records
Cacti Stats - Boost Runtime	67	Template	Cacti Stats - Boost Runtime
Cacti Stats - Boost Runtime	45	Template	Cacti Stats - Boost Runtime
Cacti Stats - Boost Table Size	55	Template	Cacti Stats - Boost Table Size
Cacti Stats - Boost Table Size	77	Template	Cacti Stats - Boost Table Size
Cacti Stats - Boost Timing Detail	56	Template	Cacti Stats - Boost Timing Detail

boost_memory

确定

TheWitness added a commit that referenced this issue on May 30, 2020

`Fixing More issues with #3549` … 72baf7b

TheWitness commented on May 30, 2020 Member

Okay. Should be all resolved now.

TheWitness added the resolved label on Jun 7, 2020

TheWitness closed this as completed on Jun 7, 2020

netniV commented on Jun 7, 2020 Member

@ddb4github and @yingbaiibm can you confirm?

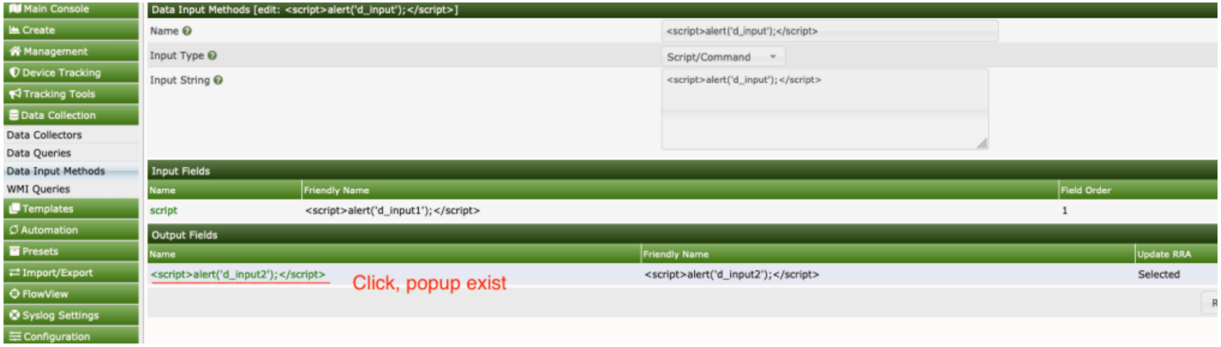
yingbaiibm commented on Jun 8, 2020

@TheWitness @netniV retest using latest code, 2 cases still have problem.

passed 4, 7, 9, 15, 16, 17, 18,

Failed 3, 19

Case#3, click a data output field has popup exist



Data Input Methods [edit: <script>alert('d_input');</script>]

Name	<script>alert('d_input');</script>
Input Type	Script/Command
Input String	<script>alert('d_input');</script>

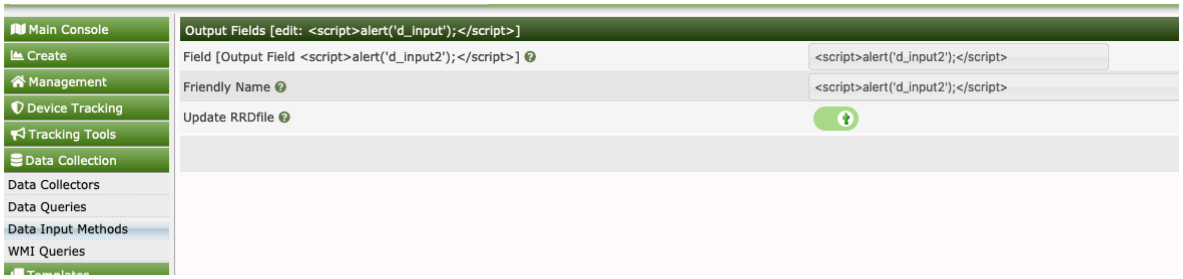
Input Fields

Name	Friendly Name	Field Order
script	<script>alert('d_input1');</script>	1

Output Fields

Name	Friendly Name	Update RRA
<script>alert('d_input2');</script>	<script>alert('d_input2');</script>	Selected

Click, popup exist



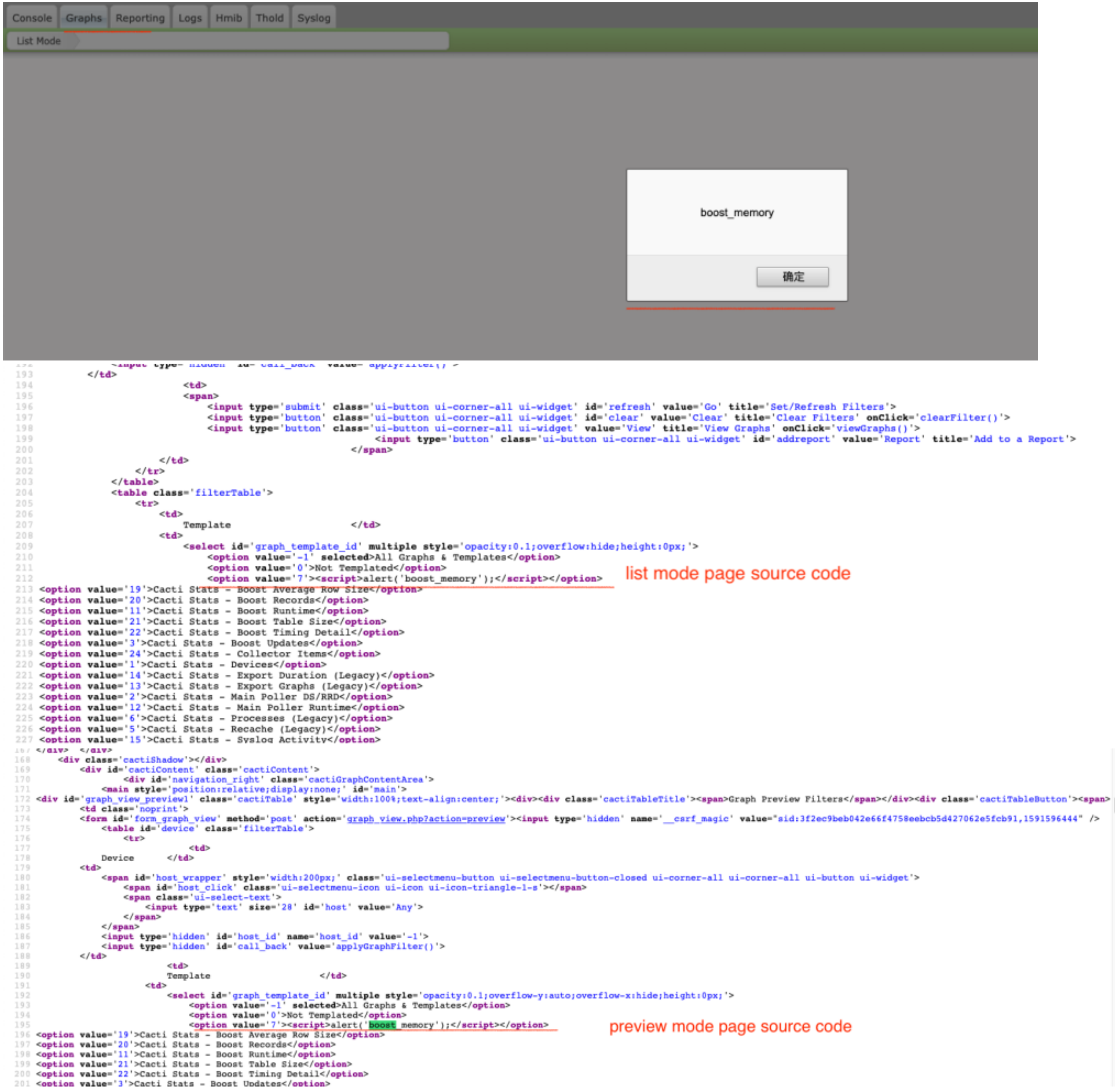
Output Fields [edit: <script>alert('d_input');</script>]

Field [Output Field <script>alert('d_input2');</script>]	<script>alert('d_input2');</script>
Friendly Name	<script>alert('d_input2');</script>
Update RRDfile	●

page source code:

```
<form class='cactiFormStart' id='data_input' name='data_input' action='data_input.php' autocomplete='off' method='post'><input type='hidden' name='__csrf_magic'
value="sid:11bcf53771bad523d8423094e203efc81d59c391,1591596622" />
<div id='data_input_field_edit1' class='cactiTable' style='width:100%;text-align:center;'><div><div class='cactiTableTitle'><span>Output Fields [edit:
&lt;script&gt;alert(&#039;d_input&#039;);&lt;/script&gt;]</span></div><div class='cactiTableButton'><span> </span></div></div><div id='data_input_field_edit1_child'
class='cactiTable'><div id='row_data_name' class='formRow odd'><div class='formColumnLeft'><div class='formFieldName'>Field [Output Field
&lt;script&gt;alert(&#039;d_input2&#039;);&lt;/script&gt;]<div class="formTooltip"><div class="cactiTooltipHint fa fa-question-circle"><span style="display:none;">Enter a name for
this Output Field <script>alert('d_input2');</script> field.  Note: If using name value pairs in your script, for example: NAME:VALUE, it is important that the name match your
output field name identically to the script output name or names.</span></div>
```

Case#19 Go to graph list view/preview mode has popup exist



```
      <input type='hidden' id='call_back' value='applyFilter()'>
        </td>
                        <td>
                        <span>
                            <input type='submit' class='ui-button ui-corner-all ui-widget' id='refresh' value='Go' title='Set/Refresh Filters'>
                            <input type='button' class='ui-button ui-corner-all ui-widget' id='clear' value='Clear' title='Clear Filters' onClick='clearFilter()'>
                            <input type='button' class='ui-button ui-corner-all ui-widget' value='View' title='View Graphs' onClick='viewGraphs()'>
                                                <input type='button' class='ui-button ui-corner-all ui-widget' id='addreport' value='Report' title='Add to a Report'>
                                            </span>
                    </td>
                </tr>
            </table>
            <table class='filterTable'>
                <tr>
                    <td>
                        Template                        </td>
                    <td>
                        <select id='graph_template_id' multiple style='opacity:0.1;overflow:hide;height:0px;'>
                            <option value='-1' selected>All Graphs & Templates</option>
                            <option value='0'>Not Templated</option>
                            <option value='7'><script>alert('boost_memory');</script></option>
<option value='19'>Cacti Stats - Boost Average Row Size</option>
<option value='20'>Cacti Stats - Boost Records</option>
<option value='11'>Cacti Stats - Boost Runtime</option>
<option value='21'>Cacti Stats - Boost Table Size</option>
<option value='22'>Cacti Stats - Boost Timing Detail</option>
<option value='3'>Cacti Stats - Boost Updates</option>
<option value='24'>Cacti Stats - Collector Items</option>
<option value='1'>Cacti Stats - Devices</option>
<option value='14'>Cacti Stats - Export Duration (Legacy)</option>
<option value='13'>Cacti Stats - Export Graphs (Legacy)</option>
<option value='2'>Cacti Stats - Main Poller DS/RRD</option>
<option value='12'>Cacti Stats - Main Poller Runtime</option>
<option value='6'>Cacti Stats - Processes (Legacy)</option>
<option value='5'>Cacti Stats - Recache (Legacy)</option>
<option value='15'>Cacti Stats - Syslog Activity</option>
```

list mode page source code

```
</div>  </div>
    <div class='cactiShadow'></div>
        <div id='cactiContent' class='cacticontent'>
                <div id='navigation_right' class='cactiGraphContentArea'>
            <main style='position:relative;display:none;' id='main'>
<div id='graph_view_preview1' class='cactiTable' style='width:100%;text-align:center;'><div><div class='cactiTableTitle'><span>Graph Preview Filters</span></div><div class='cactiTableButton'><span>
        <td class='noprint'>
        <form id='form_graph_view' method='post' action='graph_view.php?action=preview'><input type='hidden' name='__csrf_magic' value="sid:3f2ec9beb042e66f4758eebcb5d427062e5fcb91,1591596444" />
            <table id='device' class='filterTable'>
                <tr>
                            <td>
            Device      </td>
        <td>
            <span id='host_wrapper' style='width:200px;' class='ui-selectmenu-button ui-selectmenu-button-closed ui-corner-all ui-corner-all ui-button ui-widget'>
                <span id='host_click' class='ui-selectmenu-icon ui-icon ui-icon-triangle-1-s'></span>
                <span class='ui-select-text'>
                    <input type='text' size='28' id='host' value='Any'>
                </span>
            </span>
            <input type='hidden' id='host_id' name='host_id' value='-1'>
            <input type='hidden' id='call_back' value='applyGraphFilter()'>
        </td>
                        <td>
                        Template                        </td>
                    <td>
                        <select id='graph_template_id' multiple style='opacity:0.1;overflow-y:auto;overflow-x:hide;height:0px;'>
                            <option value='-1' selected>All Graphs & Templates</option>
                            <option value='0'>Not Templated</option>
                            <option value='7'><script>alert('boost_memory');</script></option>
<option value='19'>Cacti Stats - Boost Average Row Size</option>
<option value='20'>Cacti Stats - Boost Records</option>
<option value='11'>Cacti Stats - Boost Runtime</option>
<option value='21'>Cacti Stats - Boost Table Size</option>
<option value='22'>Cacti Stats - Boost Timing Detail</option>
<option value='3'>Cacti Stats - Boost Updates</option>
```

preview mode page source code

netniV commented on Jun 8, 2020 Member

Thanks for the feedback, we will look into it again.

netniV reopened this on Jun 8, 2020

netniV added a commit that referenced this issue on Jun 8, 2020

Further XSS fixes for #3549 de5e60c

netniV commented on Jun 8, 2020 Member

I believe that these two should be resolved now. Can you retest for me? Thank you so much for your time and patience.

yingbaiibm commented on Jun 8, 2020

@netniV test using your new fix. passed for data_input case.
For graph -preview mode, still has popup exist. please have a check.

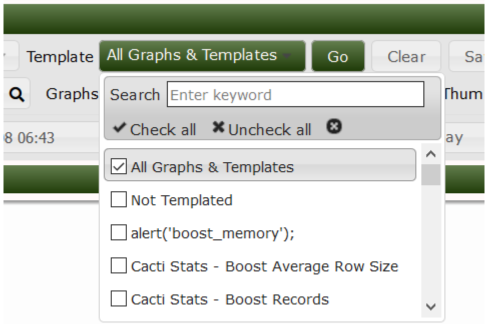
netniV commented on Jun 8, 2020 • edited Member

I tried to reproduce it and the with my fix I seemed to no longer have the error. Can you give the page/mode you are using?

ddb4github commented on Jun 8, 2020 • edited Contributor Author

> I tried to reproduce it and the with my fix I seemed to no longer have the error. Can you give the page/mode you are using?

Under Preview mode, 'alert' come from `Template` filter that is generated by function `html_graph_preview_filter`



ddb4github pushed a commit to ddb4github/cacti that referenced this issue on Jun 8, 2020

`Fixed: Cacti#3549 XSS under graph preview mode` 709a89c

netniV pushed a commit that referenced this issue on Jun 8, 2020

`Fixed: #3549 XSS under graph preview mode (#3600)` ··· a3233a1

netniV commented on Jun 8, 2020 Member

Thanks for the PR. Saves me doing the same thing. I think I fixed it under somewhere else.

TheWitness commented on Jun 13, 2020 Member

Okay, looks like this is good then. Stored XSS makes peoples lives more interesting I guess.

TheWitness closed this as completed on Jun 13, 2020

TheWitness added a commit that referenced this issue on Jun 13, 2020

`Issue #3549` ··· 80ec47b

TheWitness commented on Jun 13, 2020 Member

Found one more in lib/import.php.

netniV changed the title ~~Several XSS Vulnerabilities~~ **Lack of escaping on some pages can lead to XSS exposure** on Jul 12, 2020

github-actions bot locked and limited conversation to collaborators on Oct 10, 2020

Assignees

No one assigned

Labels

bug resolved SECURITY

Projects

None yet

Milestone

1.2.13

Development

No branches or pull requests

4 participants