New issue

Jump to bottom

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

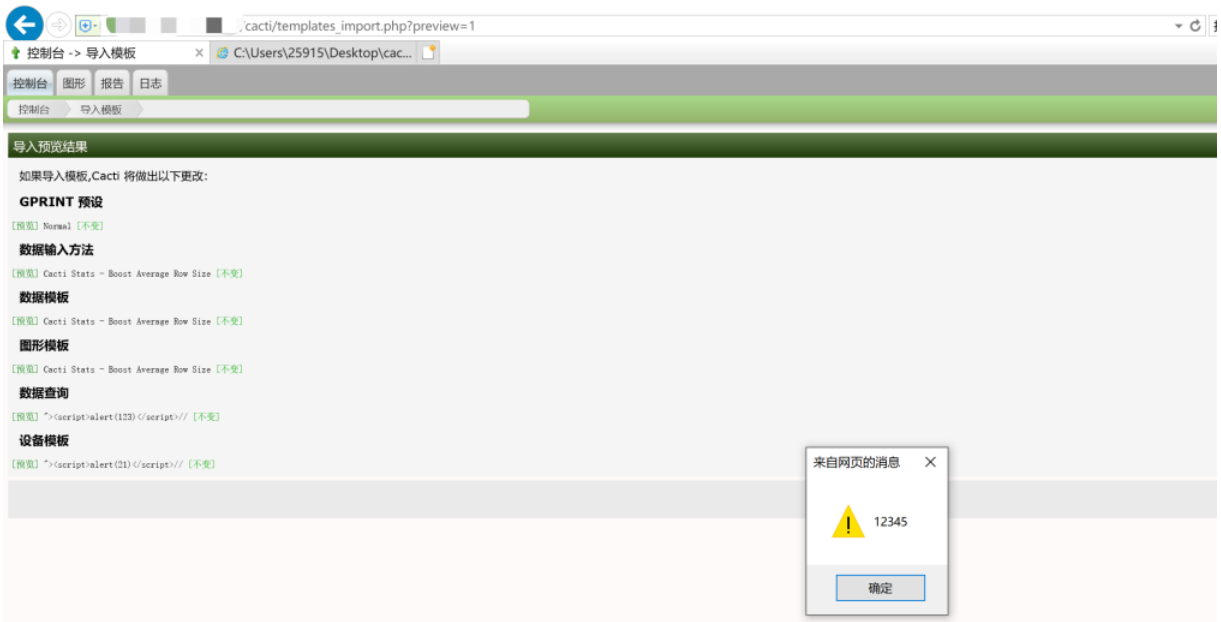
Closed **joelister** opened this issue on Jul 24, 2020 · 1 comment

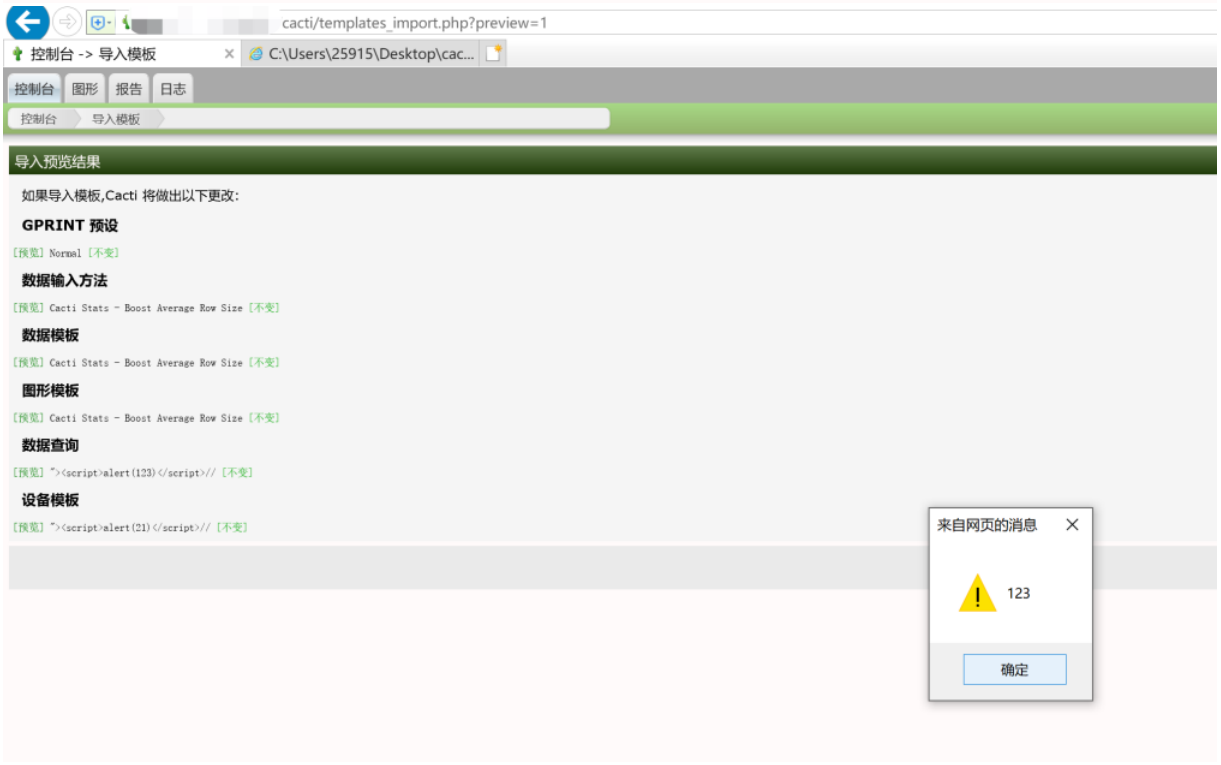
Labels bug confirmed SECURITY

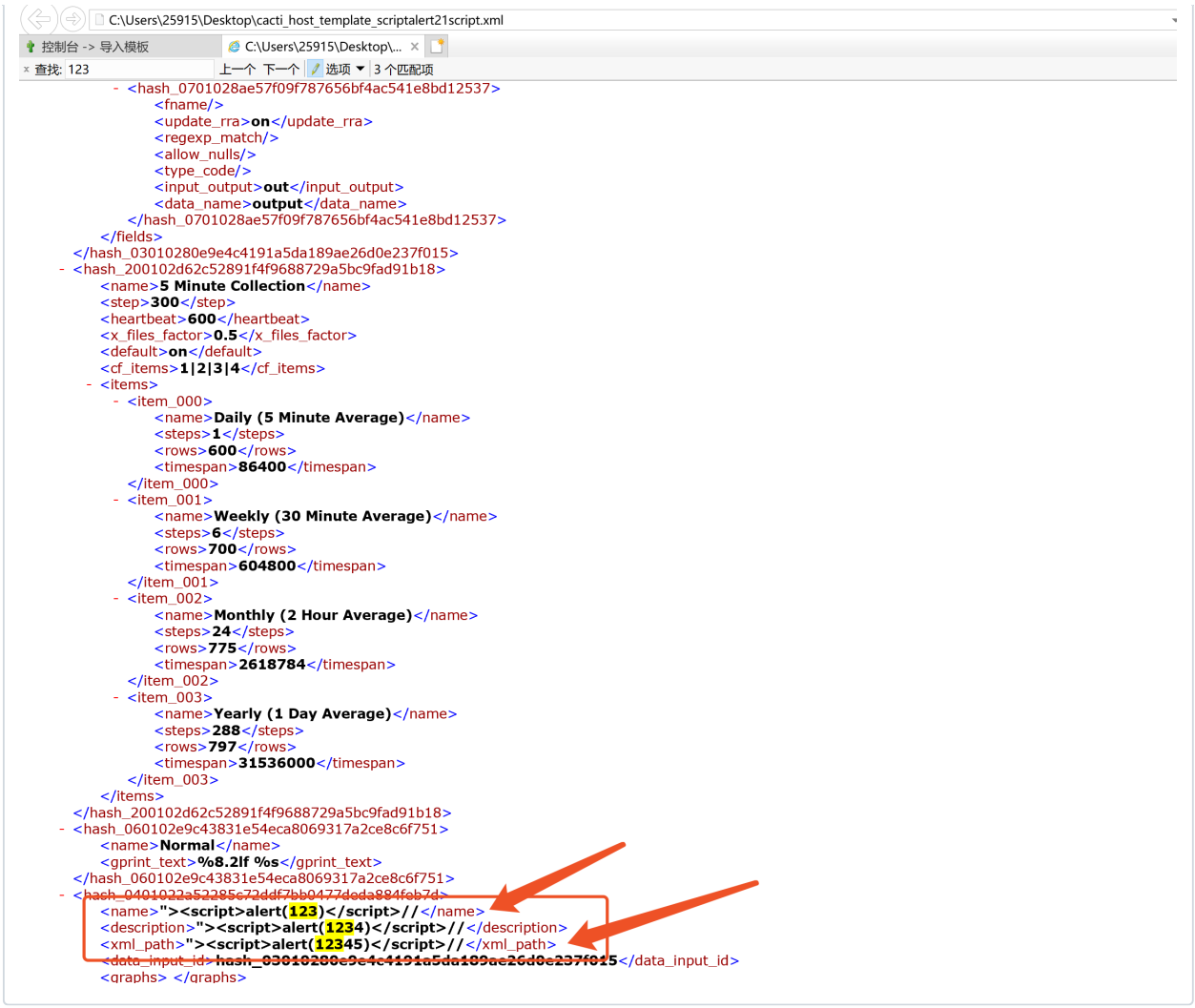
Milestone v1.2.14

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


cacti/templates_import.php?preview=1
控制台 -> 导入模板
C:\Users\25915\Desktop\cac...
控制台
图形
报告
日志
控制台
导入模板
导入预览结果
如果导入模板,Cacti 将做出以下更改:
GPRINT 预设
[预览] Normal [不变]
数据输入方法
[预览] Cacti Stats - Boost Average Row Size [不变]
数据模板
[预览] Cacti Stats - Boost Average Row Size [不变]
图形模板
[预览] Cacti Stats - Boost Average Row Size [不变]
数据查询
[预览] "><script>alert(123)</script>// [不变]
设备模板
[预览] "><script>alert(21)</script>// [不变]
来自网页的消息
12345
确定


cacti/templates_import.php?preview=1
控制台 -> 导入模板
C:\Users\25915\Desktop\cac...
控制台
图形
报告
日志
控制台
导入模板
导入预览结果
如果导入模板,Cacti 将做出以下更改:
GPRINT 预设
[预览] Normal [不变]
数据输入方法
[预览] Cacti Stats - Boost Average Row Size [不变]
数据模板
[预览] Cacti Stats - Boost Average Row Size [不变]
图形模板
[预览] Cacti Stats - Boost Average Row Size [不变]
数据查询
[预览] "><script>alert(123)</script>// [不变]
设备模板
[预览] "><script>alert(21)</script>// [不变]
来自网页的消息
123
确定



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 so. 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