Bug 1896695 (CVE-2020-25706) - CVE-2020-25706 cacti: Improper escaping of error message leads to XSS during template import preview

Keywords:	Security ×	**Reported:**	2020-11-11 10:06 UTC by Michael Kaplan
Status:	CLOSED NOTABUG	**Modified:**	2021-10-28 05:27 UTC (History)
Alias:	CVE-2020-25706	**CC List:**	3 users (show)
Product:	Security Response	**Fixed In Version:**	cacti 1.2.14
Component:	vulnerability	**Doc Type:**	---
Version:	unspecified	**Doc Text:**	A Cross-site scripting (XSS) flaw was found in Cacti in the templates_import.php, caused by an improper escaping of error message during the template import preview in the xml_path field. The highest threat from this vulnerability is to confidentiality and integrity.
Hardware:	All	**Clone Of:**	
OS:	Linux	**Environment:**	
Priority:	medium	**Last Closed:**	2021-10-28 05:27:39 UTC
Severity:	medium		
Target Milestone:	---		
Assignee:	Red Hat Product Security		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:			
Blocks:			
TreeView+	depends on / blocked		

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Michael Kaplan 2020-11-11 10:06:19 UTC — Description

```
A cross-site scripting (XSS) vulnerability exists in templates_import.php (Cacti
1.2.13) due to Improper escaping of error message during template
import preview in the xml_path field
```

Michael Kaplan 2020-11-11 10:06:25 UTC — Comment 1

```
Acknowledgments:

Name: listerjoe
```

Michael Kaplan 2020-11-11 10:06:52 UTC — Comment 3

```
External References:

https://github.com/Cacti/cacti/issues/3723
https://github.com/Cacti/cacti/commit/39458efcd5286d50e6b7f905fedcdc1059354e6e
```

Note

You need to log in before you can comment on or make changes to this bug.