New issue

Jump to bottom

Remote Code Execution due to input validation failure in Performance Boost Debug Log (CVE-2020-7237) #3201

Closed **0xfatty** opened this issue on Jan 19, 2020 · 2 comments

Labels bug resolved SECURITY

0xfatty commented on Jan 19, 2020 • edited

Describe the bug
An input validation error found in Boost Debug Log field leads to Remote Code Execution.

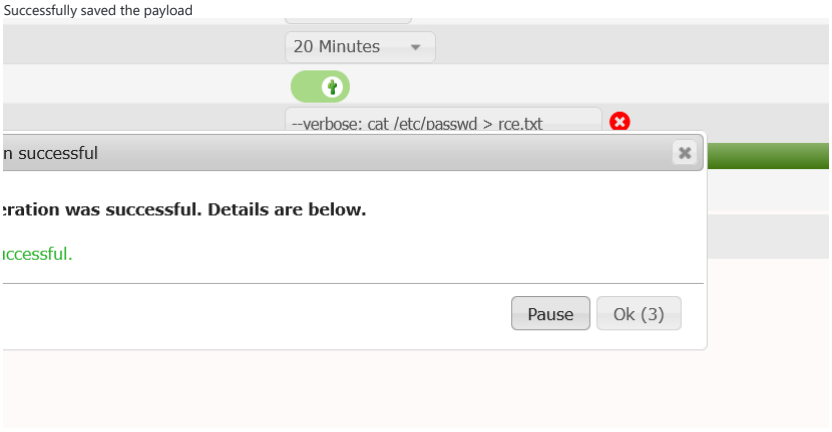
To Reproduce
Steps to reproduce the behavior:

1. Navigate to Console -> Configuration -> Settings -> Performance
2. In Boost Debug Log field, type in the payload:
   `--verbose; cat /etc/passwd > rce.txt`
3. Save. Even the $input_whitelisting in config.php is ON, it would still accept this payload.
4. Wait a little bit until new polling cycle gets fetched. Navigate to `http://cacti/rce.txt` to see /etc/passwd content.

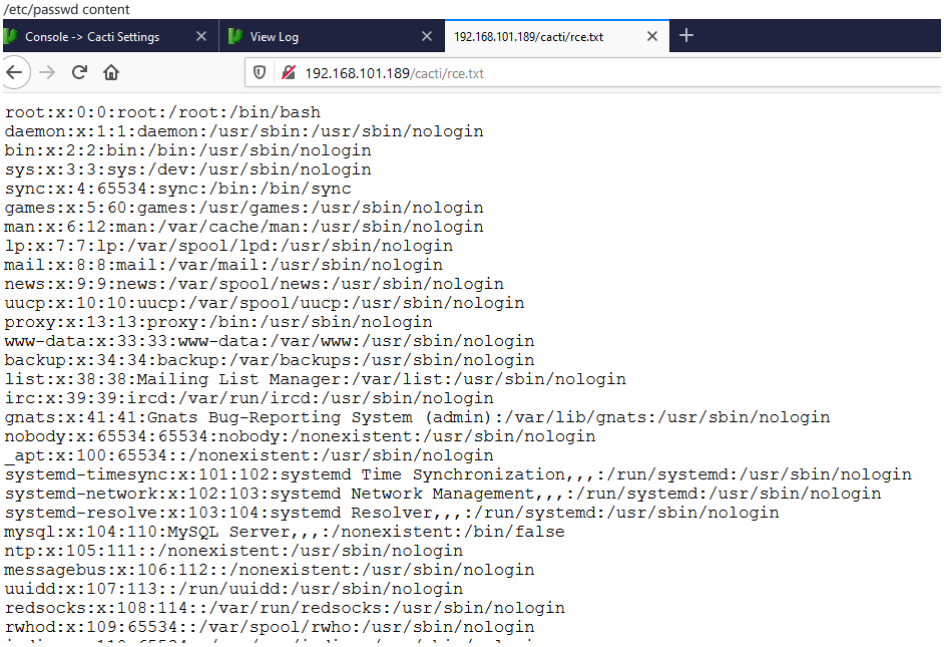
Screenshots

- Payload

- Successfully saved the payload



- /etc/passwd content



Root cause

- Not like other fields in Configuration tab, Boost Debug Log would still be saved even if the input contains special characters.
- Tracing back to server log, I observed that this is being handled by poller_automation.php where it gets fetched by the poller process.
- Taking a look at the poller_automation.php, I observed that there are 5 different arguments that can be used to passed into its command. Hence, we can use either --debug, --force, --verbose, --version, or --help to pass into Boost Debug Log field.
- After crafting a payload, the script will look like:
  `/bin/php <path>/poller_automation.php --verbose; cat /etc/passwd > rce.txt` where it gets fetched by the new poller process and create rce.txt in webroot.

Remediation

- Apply a check on this field (i.e: input length, input characters)
- If this field is supposed to take these mentioned arguments, create a drop-down menu instead of string field if possible.

Please let me know if you need any further information.

Chi Tran

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

`Resolving Issue #3201` ··· `5010719`

cigamit added **bug** resolved SECURITY labels on Jan 19, 2020

cigamit commented on Jan 19, 2020 — Member

Should be all set now.

0xfatty commented on Jan 19, 2020 • edited — Author

A CVE has been assigned for this issue.

CVE-2020-7237.

I have also committed to CHANGELOG.

0xfatty pushed a commit to 0xfatty/cacti that referenced this issue on Jan 19, 2020

`Add cve to issue Cacti#3201` `ac5c973`

TheWitness pushed a commit that referenced this issue on Jan 20, 2020

`Add cve to issue #3201 (#3203)` `276789e`

TheWitness closed this as completed on Jan 23, 2020

netniV changed the title ~~Vulnerability Report: Remote Code Execution due to input validation in Performance Boost Debug Log~~ Remote Code Execution due to input validation failure in Performance Boost Debug Log (CVE-2020-7237) on Feb 9, 2020

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

3 participants