

Meethack Torino
Vulnerability Research &
Exploit Development:
Cacti - CVE-2022-46169



Cacti - CVE-2022-46169

Unauthenticated Command Injection #5119



Closed netniV opened this issue on Dec 31, 2022 · 8 comments



netniV commented on Dec 31, 2022

Member



Describe the bug

A bug exists where the proxy headers are incorrectly checked when not needed which can be used to bypass IP based security

Expected behavior

Cacti should only check the headers an admin defines as being set



<https://github.com/cacti/cacti/issues/5119>

What is Cacti?



Cacti®

Info ▾ Development ▾ Support ▾

Release 1.2.24

About Cacti

Cacti provides a robust and extensible operational monitoring and fault management framework for users around the world. Is also a complete network graphing solution designed to harness the power of [RRDTool](#)'s data storage and graphing functionality.

Cacti includes a fully distributed and fault tolerant data collection framework, advanced template based automation features for Devices, Graphs and Trees, multiple data acquisition methods, the ability to be extended through Plugins, Role based User, Group and Domain management features in addition to a theming engine and multiple language support all right out of the box.

All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with tens of thousands of devices.

[Get more details about Cacti.](#)

The screenshot displays the Cacti web interface. At the top, there is a green navigation bar with the Cacti logo and menu items: 'Graphs', 'Reporting', and 'Logs'. Below this, a left-hand navigation menu lists 'Main Console', 'Create', and 'Management'. The 'Management' section is expanded to show 'Devices', 'Sites', 'Trees', 'Graphs', and 'Data Sources'. The main content area is titled 'Devices' and features a search bar with filters for Site, Data Collector, Template, and Location. Below the search bar, a table lists device details. The table has columns for Device Description, Hostname, ID, Graphs, Data Sources, Status, In State, Uptime, Poll Time, Current (ms), Average (ms), Availability, and Created. The first row shows 'Cacti Server' with hostname 'localhost', ID '1', 4 graphs, 5 data sources, and a status of 'Up'.

Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability	Created
Cacti Server	localhost	1	4	5	Up	N/A	N/A	0.1	0	0	100 %	2020-09-06 21:43:06
Cacti (1185)	193.169.11.105	56	13	10	Up	120	12	0.26	0.25	1.15	99.26 %	2020-09-06 21:43:06

<https://www.cacti.net/>

Let's try to “discover” the exploit blindly

- We can use:
 - Issue – <https://github.com/cacti/cacti/issues/5119>
 - Vulnerable container – <https://github.com/m3ssap0/cacti-rce-cve-2022-46169-vulnerable-application>
 - Vulnerable source code – <https://github.com/Cacti/cacti/tree/release/1.2.22>
 - Fixed source code – <https://github.com/Cacti/cacti/tree/release/1.2.23>
- Let's try not to use:
 - Security advisory (contains root cause) and public exploits:
 - <https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf>
 - <https://www.exploit-db.com/exploits/51166>
 - <https://github.com/vulhub/vulhub/tree/master/cacti/CVE-2022-46169>

Local vulnerable environment

- Setup / Tear down:
 - `git clone https://github.com/m3ssap0/cacti-rce-cve-2022-46169-vulnerable-application.git`
 - `cd cacti-rce-cve-2022-46169-vulnerable-application`
 - Follow instructions reported here: <https://github.com/m3ssap0/cacti-rce-cve-2022-46169-vulnerable-application#usage>

Starting points

- Comparing branches –
<https://github.com/Cacti/cacti/compare/release/1.2.22...release/1.2.23>
- Fix commit –
<https://github.com/Cacti/cacti/commit/7f0e16312dd5ce20f93744ef8b9c3b0f1ece2216>
- Semgrep:
 - `semgrep scan`
– `--config="r/php.lang.security.exec-use.exec-use"`

Solutions:

<https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf>

<https://www.exploit-db.com/exploits/51166>

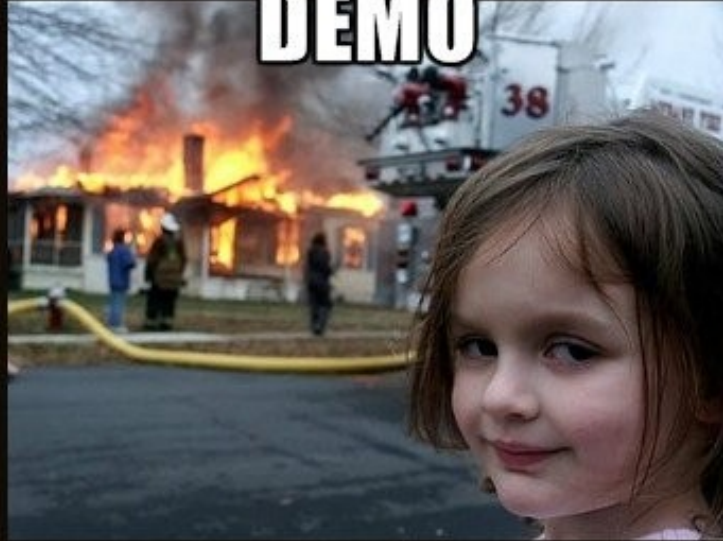


TL;DR

- AuthZ check –
https://github.com/Cacti/cacti/blob/a0a8b7d51dcbe1ac0f91788e3579ac8962ba66ad/remote_agent.php#L53
- `remote_client_authorized` –
https://github.com/Cacti/cacti/blob/a0a8b7d51dcbe1ac0f91788e3579ac8962ba66ad/remote_agent.php#L132
- `get_client_addr` –
<https://github.com/Cacti/cacti/blob/a0a8b7d51dcbe1ac0f91788e3579ac8962ba66ad/lib/functions.php#L6654>
- `polldata` action –
https://github.com/Cacti/cacti/blob/a0a8b7d51dcbe1ac0f91788e3579ac8962ba66ad/remote_agent.php#L61
- `poll_for_data` / `POLLER_ACTION_SCRIPT_PHP` / `proc_open` (*sink*) –
https://github.com/Cacti/cacti/blob/a0a8b7d51dcbe1ac0f91788e3579ac8962ba66ad/remote_agent.php#L385

Demo

**TIME FOR A LIVE
DEMO**



WHAT COULD GO WRONG?
memegenerator.net

That's all folks!

