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

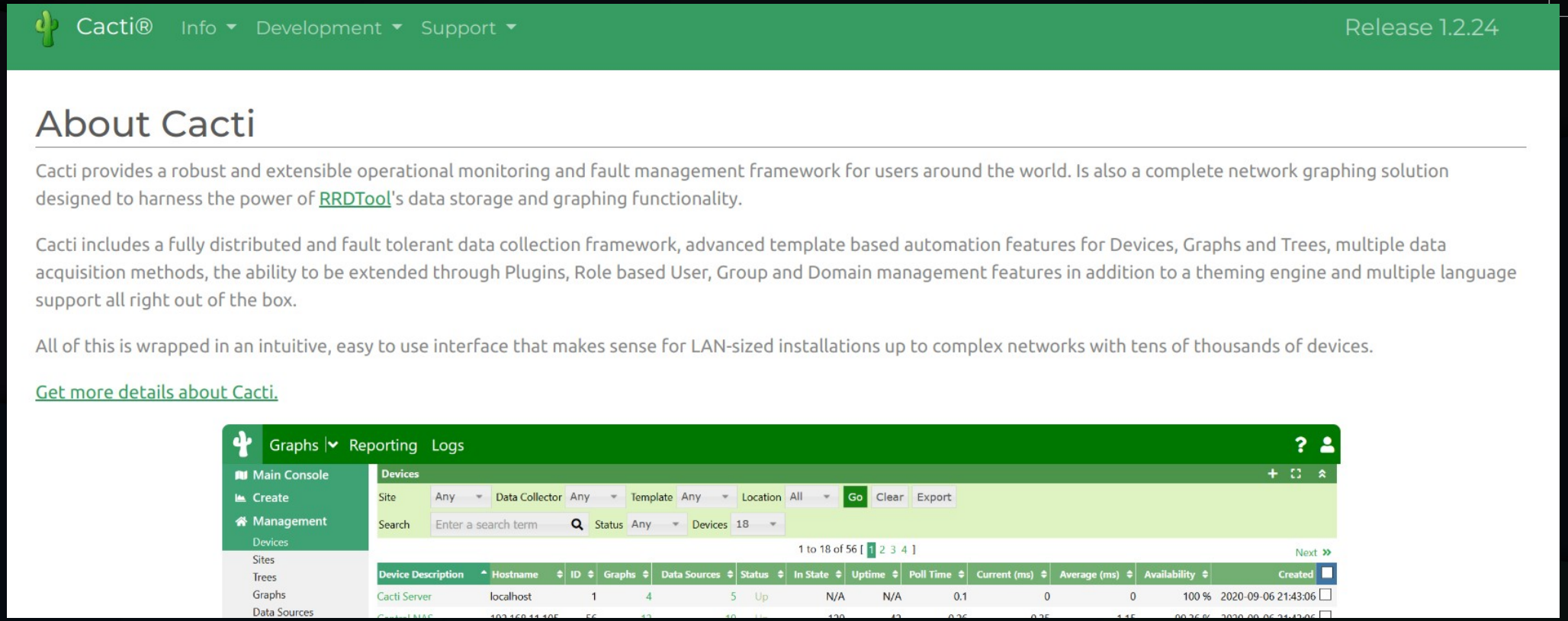
A bug exists where the proxy headers are incorrectly checked when not needed which can be used to bypass IP based security

Expected behavior

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

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

What is Cacti?



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
38
WHAT COULD GO WRONG?
memegenerator.net

That’s all folks!