OS Command Injection in Cacti

1. Advisory Information

Advisory ID: BONSAI-2010-0105
Date published: 2010-04-21
Vendors contacted: Cacti
Release mode: Coordinated release

2. Vulnerability Information

Class: Injection
Remotely Exploitable: Yes
Locally Exploitable: Yes
CVE Name: To be Defined

3. Software Description

Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features 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 hundreds of devices [0].

4. Vulnerability Description

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

For additional information, please read [1] (A1 - Injection)

5. Vulnerable packages

Version <= 0.8.7e

6. Non-vulnerable packages

New version is not available. In order to mitigate the OS Command Injection, the administrators of Cacti should trust the user who has the privileges to access to the vulnerable parts of the application. New point release of Cacti would resolve this specific issue.

7. Credits

This vulnerability was discovered by Nahuel Grisolia (nahuel -at- bonsai-sec.com).

8. Technical Description

8.1. OS Command Injection

CVSSv2 Score: 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

Cacti is prone to a remote command execution vulnerability because the software fails to adequately sanitize user-suplied input.

Successful attacks can compromise the affected software and possibly the operating system running Cacti.

The vulnerability can be triggered by any user doing:

1)

Edit or Create a Device with FQDN '**NotARealIPAddress;CMD;**' (without single quotes) and Save it.

Edit the Device again and reload any data query already created.

CMD will be executed with Web Server rights.

2)

Edit or Create a Graph Template and use as Vertical Label '**BonsaiSecLabel";CMD; "**' (without single quotes) and Save it.

Go to Graph Management section and Select it.

CMD will be executed with Web Server rights.

Note that other properties of a Graph Template might also be affected.

9. Report Timeline

- 2010-04-03 / Vulnerabilities were identified
- 2010-04-06 / Vendor Contacted
- 2010-04-17 / Vendor released a mitigation plan
- 2010-04-21 / The advisory BONSAI-2010-0105 is published

10. References

[0] http://www.cacti.net/

[1] http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

11. About Bonsai

Bonsai is a company involved in providing professional computer information security services. Currently a sound growth company, since its foundation in early 2009 in Buenos Aires, Argentina, we are fully committed to quality service, and focused on our customers real needs.

12. Disclaimer

13. Research

http://www.bonsai-sec.com/en/research/vulnerability.php