Advisory Name: Information disclosure in FreePBX 2.5.x

Internal Cybsec Advisory Id: 2010-0101

Vulnerability Class: Information disclosure

Release Date: 15/01/2010

Affected Applications: Confirmed in FreePBX 2.5.x Other versions may also be affected

Affected Platforms: Any running FreePBX2.5.x

Local / Remote: Remote

Severity: Medium – CVSS: 4 (AV:N/AC:L/Au:S/C:P/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 user with access to the "administrators" section could see other's administrators passwords by viewing the html's source code.

Proof of Concept:

In http://xx.xx.xx.xx/admin/config.php?display=ampusers&userdisplay=admin

```
<a href=# class="info">Password<span>Create a password for this new
user</span></a>:
</td><td>
<input type="password" size="20" name="password" value="admin" tabindex="2"/>
</td>
```

Impact:

A user with access to the "administrator" sections may access to other's administrators passwords.

Solution:

Update to v2.6

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