**Advisory Name:** Permanent Cross-Site Scripting (XSS) in FreePBX 2.5.x – 2.6.0

**Internal Cybsec Advisory Id:** 2010-0102

**Vulnerability Class:** Permanent Cross-Site Scripting (XSS)

**Release Date:** 15/01/2010

**Affected Applications:** Confirmed in FreePBX  2.5.x and 2.6.0 - Other versions may also be affected

**Affected Platforms:** Any running FreePBX 2.5.x and 2.6.0

**Local / Remote:** Remote

**Severity:** Medium – CVSS: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

**Researcher:** Ivan Huertas

**Vendor Status:** Patched

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

## Vulnerability Description:

A permanent Cross Site Scripting vulnerability was found in FreePBX 2.5.x and 2.6, because the application fails to sanitize user-supplied input. The vulnerability can be triggered by any logged-in user who is able to add an Inbound Route.

## Proof of Concept:

* Add <script>alert(“Cybsec XSS”);</script> as a Description in an Inbound Route.

## Impact:

An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the application.

## Solution:

Upgrade to the latest version

- http://www.freepbx.org/v2/changeset/8589
- http://www.freepbx.org/v2/changeset/8590
- http://www.freepbx.org/v2/changeset/8591

## Vendor Response:

2009-30-12 – Vulnerability was identified
2010-01-07 – Vendor contacted
2010-01-11 – Vendor confirmed vulnerability
2010-01-14 – Vendor released fixed version
2010-01-15 – Vulnerability published

## 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