Advisory Name: Multiple Permanent Cross-site Scripting in Phreebooks v2.0

Internal Cybsec Advisory Id:

Vulnerability Class: Permanent Cross-site Scripting

Release Date: 2010-05-26

Affected Applications: Phreebooks v2.0

Affected Platforms: Any running Phreebooks v2.0

Local / Remote: Remote

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

Researcher: Gustavo Sorondo

Vendor Status: N/A

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

Vulnerability Description:
Multiple permanent Cross-site Scripting vulnerabilities were found in Phreebooks v2.0, because the application fails to sanitize user-supplied input. The vulnerability can be triggered by any logged-in user who is able to add or modify Vendors, Customers, Employees or Inventary items.

Proof of Concept:

Create a new Vendor, Customer or Employee entering <script>alert(“XSS”);</script> in the Name/Company field; then browse maintain Vendors, Customers or Employees.

Or

Create a new Inventary item entering <script>alert(“XSS”);</script> in the Short Description field; then browse Inventary → Edit/Mantain

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:

N/A

Vendor Response:

2010-03-18 – Vulnerability was identified
2010-03-29 – First attempt to contact vendor
2010-05-18 – Second and last attempt to contact vendor
2010-06-08 – Vulnerability was released

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
gsorondo <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