Advisory Name: Directory Traversal in Phreebooks v2.0

Internal Cybsec Advisory Id:

Vulnerability Class: Directory Traversal

Release Date: 2010-05-26

Affected Applications: Phreebooks v2.0

Affected Platforms: Any running Phreebooks v2.0

Local / Remote: Remote

Severity: Medium – CVSS: 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Researcher: Gustavo Sorondo

Vendor Status: N/A

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

Vulnerability Description:

A vulnerability has been found in Phreebooks v2.0 which allows malicious people to access local files by entering special characters in variables used to create file paths. The attackers use "../" sequences to move up to root directory, thus permitting navigation through the file system.

Proof of Concept:

```
http://[host]/[phreebooks]/index.php?cat=../../../../../../../etc/passwd%00.
```

Impact:

Read arbitrary local files.

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