Advisory Name: Arbitrary File Download in OSSIM

Vulnerability Class: Arbitrary File Download

Release Date: 03-16-2010

Affected Applications: Confirmed in OSSIM 2.2. Other versions may also be affected.

Affected Platforms: Multiple

Local / Remote: Remote

Severity: High – CVSS: 7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N)

Researcher: Nahuel Grisolía

Vendor Status: Fixed in OSSIM 2.2.1

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

Vulnerability Description:

OSSIM is prone to a Arbitrary File Download vulnerability because the software fails to adequately sanitize user-supplied input.

The file “download.php” in “/ossiminstall/repository/” directory suffers from an Arbitrary File Download vulnerability due to the missed input validation on the "file" parameter; in particular no validation is done on path traversal patterns.

Proof of Concept:

http://192.168.2.35/ossim/repository/download.php?file=../../../../../../../../etc/passwd&name=passwd.txt

Impact:

Through this vulnerability remote and unauthenticated users could download any file accessible by the Web server and by reading source files a malicious user could read important information such as database passwords.

Solution: Fixed in OSSIM 2.2.1. See http://www.alienvault.com/community.php?section=News

Vendor Response:

02-03-2010 – Initial contact
03-11-2010 – OSSIM 2.2.1 is available

Contact Information:

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