



Advisory Name: SQL injection in OSSIM

Vulnerability Class: SQL injection

Release Date: 12-16-2009

Affected Applications: Confirmed in OSSIM 2.1.5. Other versions may also be affected.

Affected Platforms: Multiple

Local / Remote: Remote

Severity: High – CVSS: 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

Researcher: Nahuel Grisolia

Vendor Status: Acknowledged/Fixed. New release available (OSSIM 2.1.5-4)

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

Vulnerability Description:

A vulnerability has been discovered in OSSIM, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed via the "id_document" parameter to repository_attachment.php is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability is confirmed in version 2.1.5. Other versions may also be affected.

Proof of Concept:

http://XXX.XXX.XXX.XXX/ossim/repository/repository_attachment.php?id_document=1%20union%20select%201,2,login,4%20from%20users

http://XXX.XXX.XXX.XXX/ossim/repository/repository_attachment.php?id_document=1%20union%20select%201,2,pass,4%20from%20users

Impact: Execute arbitrary SQL queries.

Solution: Upgrade to OSSIM 2.1.5-4



Vendor Response:

2009-12-08 – Vulnerability is identified
2009-12-09 – Vendor is contacted
2009-12-09 – Vendor confirmed vulnerability
2009-12-16 – Vendor released fixed version
2009-12-16 – Vulnerability is published

Contact Information:

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

(c) 2009 - CYBSEC S.A. Security Systems