Advisory Name: Reflected Cross-Site Scripting (XSS) in osTicket

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

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

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 reflected Cross Site Scripting vulnerability was found in osTicket 1.6 RC5, because the application fails to sanitize user-supplied input. Any logged-in user can trigger the vulnerability.

Proof of Concept:

http://x.x.x.x/upload/scp/ajax.php?api=1%3Cscript%3Ealert%28%22xss%22%29;%3C/script%3E&f=cannedResp

http://x.x.x.x/upload/scp/ajax.php?api=kbase&f=%3Cscript%3Ealert%28%22xss%22%29;%3C/script%3E

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: 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