CYBSEC®
Security Systems

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

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

Release Date: 2010-03-09

Affected Applications: Confirmed in EGroupware 1.4.001+.002 and 1.6.001+.002. EGroupware Premium Line 9.1 and 9.2 is also affected. Other versions may also be affected.

Affected Platforms: Multiple

Local / Remote: Remote

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

Researcher: Nahuel Grisolía

Vendor Status: Acknowledged / Fixed.

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

Reference to CYBSEC Security Advisories: http://www.cybsec.com/EN/research/default.php

Vulnerability Description:

A reflected Cross Site Scripting vulnerability was found in EGroupware, because the application fails to sanitize user-supplied input. The vulnerability can be triggered by any user.

Proof of Concept:

Working on Mozilla Firefox 3.5.7:

http://server/egroupware/login.php?lang="%20style="width:100%;height:100%;display:block;position:absolute;top:0px;left:0px"%20onMouseOver="alert(document.cookie)

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: Fixed in EGroupware version 1.6.003, EPL-9.1.20100309 and EPL-9.2.20100309. Link available with information: http://www.egroupware.org/news?category_id=95&item=93

Vendor Response:

Feb 5, 2010 - CYBSEC first notification
Feb 8, 2010 between Mar 7, 2010 – Multiple contacts.
Mar 9, 2010 – Vendor released fixed versions.
Mar 9, 2010 – Vulnerability is published.

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 S.A. is devoted exclusively to provide professional services specialized in Computer Security. More than 150 clients around the globe validate our quality and professionalism.

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