



Advisory Name: Arbitrary File Upload in Achievo 1.4.2

Vulnerability Class: Arbitrary File Upload

Release Date: 12-04-2009

Affected Applications: Confirmed in Achievo 1.4.2. Other versions may also be affected.

Affected Platforms: Any running Achievo

Local / Remote: Local

Severity: Medium – CVSS: 6.8 (AV:L/AC:L/Au:S/C:C/I:C/A:C)

Researcher: Nahuel Grisolia

Vendor Status: New release available (Achievo 1.4.3)

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

Vulnerability Description:

The vulnerability is caused due to an improper check in “Document Types” section under Setup menu, allowing the upload of files with arbitrary extensions to a folder inside the Webroot. This can be exploited to e.g. execute arbitrary PHP code by uploading a specially crafted PHP script containing some kind of Web Shell.

Proof of Concept:

Select a file with any extension (including PHP) and upload it using the form. The file will be available in: <http://ACHIEVOINSTALL/modules/docmanager/doctypetemplates/myuploadedfile>

For example, we can upload “cmd.php” in our installation in localhost and execute it entering: <http://localhost/achievo-1.4.2/modules/docmanager/doctypetemplates/cmd.php>

Impact:

Direct execution of arbitrary PHP code in the Web Server.

Solution:

Update the document manager and add a new config (docmanager_allowedfiletypes) for it in /configs/docmanager.php.inc. With this config you can tell the docmanager what type of files a user can upload.



More information: http://www.achievo.org/download/releasenotes/1_4_3

Vendor Response:

2009-12-03 – Vulnerability was identified
2009-12-03 – Vendor contacted
2009-12-03 – Vendor confirmed vulnerability
2009-12-03 – Vendor released fixed version
2009-12-04 – Vulnerability 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
(c) 2009 - **CYBSEC S.A. Security Systems**