



Advisory Name: Permanent Cross-Site Scripting (XSS) in Achievo 1.4.2

Vulnerability Class: Permanent Cross-Site Scripting (XSS)

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: Remote

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

Researcher: Nahuel Grisolia

Vendor Status: New release available (Achievo version 1.4.3)

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

Vulnerability Description:

A permanent Cross Site Scripting vulnerability was found in Achievo 1.4.2, because the application fails to sanitize user-supplied input. The vulnerability can be triggered by any logged-in user who is able to add a Scheduler Category.

Proof of Concept:

* Add `<script>alert("XSS in Category");</script>` as a new category. Then, browse the Scheduler.

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:

New category is now correctly sanitized.

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