

Secunia Research: ATutor Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-10/0347.html>

From: Secunia Research (*vuln_at_secunia.com*)

Date: 10/27/05

To: vuln@secunia.com

Date: Thu, 27 Oct 2005 16:56:25 +0200

Secunia Research 27/10/2005

– ATutor Multiple Vulnerabilities –

Table of Contents

Affected Software.....	1
Severity.....	2
Vendor's Description of Software.....	3
Description of Vulnerabilities.....	4
Solution.....	5
Time Table.....	6
Credits.....	7
About Secunia.....	8
Verification.....	9

1) Affected Software

ATutor 1.5.1-pl1

Other versions may also be affected.

2) Severity

Rating: Highly critical

Impact: System access, exposure of sensitive information, and
cross-site scripting

Where: Remote

3) Vendor's Description of Software

SecurityFocus Bugtraq: Secunia Research: ATutor Multiple Vulnerabilities

ATutor is an Open Source Web-based Learning Content Management System (LCMS) designed with accessibility and adaptability in mind.

Product link:

<http://atutor.ca/>

4) Description of Vulnerabilities

Secunia Research has discovered some vulnerabilities in ATutor, which can be exploited by malicious people to conduct cross-site scripting attacks, disclose sensitive information, and compromise a vulnerable system.

1) Input passed to the "addslashes", "asc", and "desc" parameters in "include/html/forum.inc.php" isn't properly verified, before it is used to create a function call. This can be exploited to call an arbitrary PHP function with an arbitrary parameter (e.g. execute arbitrary shell commands with the "exec" function).

Examples:

```
http://[host]/include/html/forum.inc.php?  
addslashes=[function]&asc=[parameter]
```

```
http://[host]/include/html/forum.inc.php?  
addslashes=[function]&desc=[parameter]
```

Successful exploitation requires that "register_globals" is enabled.

2) Input passed to the "section" parameter in "body_header.inc.php" and "print.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from local resources.

Examples:

```
http://[host]/documentation/common/body_header.inc.php?  
section=[file]%00
```

```
http://[host]/documentation/common/print.php?section=[file]%00
```

Successful exploitation requires that "register_globals" is enabled and that "magic_quotes_gpc" is disabled.

3) Input passed to the "_base_href" parameter in "admin/translate.php", the "_base_path" parameter in "include/html/editor_tabs/news.inc.php", and the "p" parameter in "documentation/add_note.php" isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities have been confirmed in version 1.5.1-p11. Other versions may also be affected.

5) Solution

Apply patch.

<http://atutor.ca/view/3/6158/1.html>

The fixes will also be included in the upcoming 1.5.2 version.

6) Time Table

10/10/2005 – Vulnerability discovered.

11/10/2005 – Vendor notified.

27/10/2005 – Vendor releases patch.

27/10/2005 – Public disclosure.

7) Credits

Discovered by Andreas Sandblad, Secunia Research.

8) About Secunia

Secunia collects, validates, assesses, and writes advisories regarding all the latest software vulnerabilities disclosed to the public. These advisories are gathered in a publicly available database at the Secunia website:

<http://secunia.com/>

Secunia offers services to our customers enabling them to receive all relevant vulnerability information to their specific system configuration.

Secunia offers a FREE mailing list called Secunia Security Advisories:

http://secunia.com/secunia_security_advisories/

9) Verification

Please verify this advisory by visiting the Secunia website:

http://secunia.com/secunia_research/2005-55/advisory/
