PHP-Nuke *cat* Old Articles Block SQL Injection

2007-01-17 23:28:52 by Raven

SECUNIA ADVISORY ID: SA23748

VERIFY ADVISORY: http://secunia.com/advisories/23748/

CRITICAL: Moderately critical

IMPACT: Manipulation of data, Exposure of sensitive information product/2385/

DESCRIPTION: Paisterist has discovered a vulnerability in PHP-Nuke, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed to the "cat" parameter through index.php to blocks/block-Old_Articles.php is not properly sanitised before being used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation e.g. allows retrieval of administrator usernames and password hashes, but requires that "register_globals" is enabled, "magic_quotes_gpc" is disabled, and the attacker knows the prefix for the database tables. The vulnerability is confirmed in version 7.9. Other versions may also be affected.

SOLUTION: Edit the source code to ensure that input is properly sanitised. Use another product.

PROVIDED AND/OR DISCOVERED BY: Paisterist

ORIGINAL ADVISORY: http://www.neosecurityteam.net/advisories/PHP-Nuke-7.9-Old-Articles-Block-cat-SQL-Injection-vulnerability-31.html

https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=2664