PHP-Nuke HTTP *referer* SQL Injection Vulnerability

2007-02-22 02:25:31 by Raven

SECUNIA ADVISORY ID: SA24224

VERIFY ADVISORY: http://secunia.com/advisories/24224/

CRITICAL: Moderately critical

IMPACT: Manipulation of data

WHERE: >From remote

SOFTWARE:
PHP-Nuke 8.x - http://secunia.com/product/13524/
PHP-Nuke 7.x - http://secunia.com/product/2385/
PHP-Nuke 6.x - http://secunia.com/product/329/
PHP-Nuke 5.x - http://secunia.com/product/689/

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

Input passed via the "referer" HTTP header in index.php is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. The vulnerability is confirmed in version 7.9 and reported in version 8.0. Other versions may also be affected.

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

PROVIDED AND/OR DISCOVERED BY: Maciej "krasza" Kukla