

[VulnWatch] PHP-Nuke mail CRLF Injection vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-12/0023.html>

From: Ulf Harnhammar (ulfh@update.uu.se)

Date: 12/20/02

Date: Fri, 20 Dec 2002 11:32:21 +0100 (CET)

From: Ulf Harnhammar <ulfh@update.uu.se>

To: bqtraq@securityfocus.com, vulnwatch@vulnwatch.org, full-disclosure@lists.netsys.com

PHP-Nuke mail CRLF Injection vulnerabilities

PROGRAM: PHP-Nuke

VENDOR: Fransisco Burzi et al.

Homepage: <http://phpnuke.org/>

VULNERABLE VERSIONS: 6.0 (the only supported version)

IMMUNE VERSIONS: 6.0 with my patch applied

LOGIN REQUIRED: no

DESCRIPTION:

"PHP-Nuke is a Web portal and online community system which includes Web-based administration, surveys, access statistics, user customizable boxes, a themes manager for registered users, friendly administration GUI with graphic topic manager, the ability to edit or delete stories, an option to delete comments, a moderation system, referer tracking, integrated banner ad system, search engine, backend/headlines generation (RSS/RDF format), Web directory like Yahoo, events manager, and support for 20+ languages."

(direct quote from the program's project page at Freshmeat)

PHP-Nuke is published under the terms of the GNU General Public License. It is a very popular program with lots and lots of installations. It is included as one of the packages in Debian GNU/Linux and one of FreeBSD's ports.

Despite all this, the program has a bad reputation regarding security matters.

SUMMARY:

PHP-Nuke has got four functions that allow restricted sending of e-mails: Feedback, Recommend Us, Send (news item) to a Friend and

VulnWatch: [VulnWatch] PHP–Nuke mail CRLF Injection vulnerabilities

Send this Journal to a Friend. They either restrict who you can send e-mails to or what message you can send to them. They are open for anonymous users as well as regular users.

By submitting special data, an attacker can escape these restrictions and use someone else's PHP–Nuke installation to send HTML e-mails to any recipient with any message that they like.

TECHNICAL DETAILS:

The fourth parameter to PHP's mail() function contains the additional mail headers that PHP doesn't have a special parameter for. In this case, it's used to add From and Reply–To headers. When PHP–Nuke constructs the value for this parameter, it doesn't check the form data it's using for CR and LF characters. As a result, an attacker can supply extra mail headers and even an extra mail body, and they will be included in the mail between the real headers and the real body. This is done by simply including CR and LF characters in the form data field that contains your e-mail address. If the attacker includes an HTML message ending with a "<!--" tag or a "" tag that sets the foreground colour to the background colour, the real mail body will not be shown in many programs.

COMMUNICATION WITH VENDOR:

I didn't contact the vendor, as Fransisco has a very bad track record when it comes to replying to security reports.

MY "SECURITY HARDENING PACKAGE":

Instead I wrote an unofficial patch for this issue. I have patched against version 6.0.

The patch simply replaces all CR and LF characters in the vulnerable variables with spaces, and then the exploit doesn't work anymore.

```
// Ulf Harnhammar  
VSU Security  
ulfh@update.uu.se
```

"I saw the worst minds of my generation / getting their political information from tabloids / listening to Savage Garden's greatest hits / getting married and having kids at 25 just 'cause the neighbours did / and building the worst administrative web-based members interface ever known to man" (To B.)

VulnWatch: [VulnWatch] PHP-Nuke mail CRLF Injection vulnerabilities

- TEXT/PLAIN attachment: [php-nuke_mail_crlf.patch](#)