

[UNIX] Apache mod_proxy_ftp Undefined Charset UTF-7 XSS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00023.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 14 Jan 2008 20:28:28 +0200
-

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Apache mod_proxy_ftp Undefined Charset UTF-7 XSS Vulnerability

SUMMARY

The Apache HTTP Server Project is "an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache has been the most popular web server on the Internet since April 1996. The November 2005 Netcraft Web Server Survey found that more than 70% of the web sites on the Internet are using Apache, thus making it more widely used than all other web servers combined".

<http://httpd.apache.org/docs/2.2/mod/mod_proxy_ftp.html> Mod_proxy_ftp "provides support for the proxying FTP sites. Note that FTP support is currently limited to the GET method." A XSS(UTF7) exist in mod_proxy_ftp.c Charset is not defined and we can provide XSS attack using ";" char in URL by setting Charset to UTF-7.

DETAILS

[UNIX] Apache mod_proxy_ftp Undefined Charset UTF-7 XSS Vulnerability

Vulnerable Systems:

- * Apache version 2.2.x with mod_proxy_ftp
- * Apache version 2.0.x with mod_proxy_ftp
- * Apache version 1.3.x with mod_proxy_ftp

Immune Systems:

- * Apache version 2.2.7-dev with mod_proxy_ftp
- * Apache version 2.0.62-dev with mod_proxy_ftp
- * Apache version 1.3.40-dev with mod_proxy_ftp

mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0005>>
CVE-2008-0005

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sp3x@xxxxxxxxxxxxxxxxxxxxxx>>
sp3x.

The original article can be found at:

<http://securityreason.com/achievement_securityalert/46>
http://securityreason.com/achievement_securityalert/46

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

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.