

Exim 3.34 and lower.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-02/0205.html>

From: Ehud Tenenbaum (analyzer@2xss.com)

Date: 02/14/02

Date: Thu, 14 Feb 2002 10:07:47 +0200
From: Ehud Tenenbaum <analyzer@2xss.com>
To: vuln-dev@securityfocus.com

Hey,

Its a good time to announce that 2xs security LTD. decided to create a research team in order to focus on finding new bugs, further more we managed to develop a security tool to discover bugs/security flaws. In the near future, the tool itself will become an open source project.

Its looks like there is few insecure/lame programming in exim mail server up to current version.

first lets take a look at the file:

```
[2xs:root:~] ls -la /usr/exim/bin/exim
-rws--x--x 1 root root 2061186 Oct 23 12:56
/usr/exim/bin/exim*
[2xs:root:~]
```

Suid goodie.

```
[2xs:w00p:/root] id
uid=1001(w00p) gid=100(users) groups=100(users)
[2xs:w00p:/root] /usr/exim/bin/exim -F `perl -e' print "A" x 32770` -C
`perl -e' print "A" x 32768`
Segmentation fault
[2xs:w00p:/root]
```

Many other argument should work as well (as long there is -C among them)

```
[2xs:root:~] gdb /usr/exim/bin/exim
GNU gdb 5.0
Copyright 2000 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you
are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
```

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

There is absolutely no warranty for GDB. Type "show warranty" for details.

This GDB was configured as "i386-slackware-linux"...

```
(gdb) r -F `perl -e' print "A" x 32770` -C `perl -e' print "A" x 32768`
```

```
Starting program: /usr/exim/bin/exim -F `perl -e' print "A" x 32770` -C `perl -e' print "A" x 32768`
```

Program received signal SIGSEGV, Segmentation fault.

```
strcpy (dest=0x820e208 'A' <repeats 200 times>..., src=0xbfff7b48 'A' <repeats 200 times>...)
```

```
  at ../sysdeps/generic/strcpy.c:40
```

```
40 ../sysdeps/generic/strcpy.c: No such file or directory.
```

```
(gdb) info registers
```

```
eax 0x48216641 1210148417
ecx 0x482166bf 1210148543
edx 0xbffa941 -1073764031
ebx 0xbfff8d4 -1073809196
esp 0xbffeeefc 0xbffeeefc
ebp 0xbffeef00 0xbffeef00
esi 0x820e208 136372744
edi 0x3 3
eip 0x401690e4 0x401690e4
eflags 0x10286 66182
cs 0x23 35
ss 0x2b 43
ds 0x2b 43
es 0x2b 43
fs 0x0 0
gs 0x0 0
fctrl 0x37f 895
fstat 0x0 0
ftag 0xffff 65535
fiseg 0x23 35
fioff 0x4009ca84 1074383492
foseg 0x2b 43
fooff 0x400fa440 1074766912
fop 0x49b 1179
```

after short debugging we found that there is no overflow since the eip register coredumped in the code segment and not in the data segment, yet we believe that there might be a way to exploit this bug with log_write(), we are not going to deliver a working exploit until the vendor will research and fix this bug.

We provide a patch to version 3.34 that should solve this bug.

In version 3.21 and lower there is another small bug with -t flag again non exploitable just bad programming.

Exim 3.34 and lower.

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

This bug was found by The Analyzer, Izik and Mixer. 2xs security research team.

should anyone have questions or comments you can email us:

analyzer@2xss.com

izik@2xss.com

mixer@2xss.com

Author reply:

This report is particularly timely, as I'm working towards releasing Exim 4 before the end of the month (a pre-release is available), so I can check these things up in the new release as well.

Thanks for running this check.

Regards,
Philip
(Author of Exim)

2xs Security team apologize to the author of exim for not mailing him first,
in the future we will notify the author/vendors before publishing bugs.

Short explanation about the patch:

On Thu, 14 Feb 2002, Matthias Andree wrote:

```
> > +strncpy(last_message_id, message_id, MESSAGE_ID_LENGTH); /* Fixed a one-byte overflow --  
2xs Security Team. */
```

```
> It's the wrong fix, suffering from the one central common strncpy  
> pitfall: strncpy has quite different semantics from strcpy: if  
> message_id meets or exceeds MESSAGE_ID_LENGTH, then last_message_id will  
> NOT be NUL-terminated (it's not a C string any more), and the function  
> that uses last_message_id is exposed to unknown risks, like running off  
> the end of the string, reading garbage, causing a segfault, whatever.
```

Well, strncpy includes the terminating \0 from the source unless there is not enough space in dest. But even when it is cut off, there will be one \0 at the end of the dest string, since last_message_id is MESSAGE_ID_LENGTH+1 bytes big, so there will always be at least one \0 .

```
> Better use strcpy, look here:
```

we'd have used strcpy or anything faster than strncpy,
if it was implemented on every platform.

```
diff -Nru exim-3.34/src.old/accept.c exim-3.34/src/accept.c  
--- exim-3.34/src.old/accept.c Tue Feb 12 13:40:44 2002
```

Exim 3.34 and lower.

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

```
+++ exim-3.34/src/accept.c Tue Feb 12 13:47:33 2002
@@ -1506,7 +1506,7 @@
```

```
/* Save for comparing with next one */
```

```
-strcpy(last_message_id, message_id);
+strncpy(last_message_id, message_id, MESSAGE_ID_LENGTH); /* Fixed a
one-byte overflow -- 2xs Security team */
```

```
/* Add the current message id onto the current process info string if
it will fit. */
```

```
diff -Nru exim-3.34/src.old/deliver.c exim-3.34/src/deliver.c
--- exim-3.34/src.old/deliver.c Tue Feb 12 13:40:44 2002
+++ exim-3.34/src/deliver.c Tue Feb 12 14:15:53 2002
@@ -3704,7 +3704,7 @@
the message size. */
```

```
deliver_force = forced;
-strcpy(message_id, id);
+strncpy(message_id, id, MESSAGE_ID_LENGTH);
return_count = 0;
message_size = 0;
```

```
@@ -4083,7 +4083,8 @@
slen += 3;
}
```

```
- strcpy(h->text + slen, s);
+ /* Fixed potential remote vulnerability -- 2xs Security team. */
+ strncpy(h->text + slen, s, size-slen-1);
slen += len;
}
```

```
diff -Nru exim-3.34/src.old/host.c exim-3.34/src/host.c
--- exim-3.34/src.old/host.c Tue Feb 12 13:40:44 2002
+++ exim-3.34/src/host.c Tue Feb 12 19:19:52 2002
@@ -281,7 +281,7 @@
}
```

```
sender_fullhost =
- store_malloc((int)strlen(fullhost) + (int)strlen(rcvhost) + 2);
+ store_malloc((int)strlen(fullhost) + (int)strlen(rcvhost) + 3);
sender_rcvhost = sender_fullhost + (int)strlen(fullhost) + 1;
strcpy(sender_fullhost, fullhost);
strcpy(sender_rcvhost, rcvhost);
@@ -471,7 +471,7 @@
```

```
next = store_malloc(sizeof(ip_address_item));
next->next = NULL;
- strcpy(next->address, s);
+ strncpy(next->address, s, 46);
```

Exim 3.34 and lower.

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

```
    if (yield == NULL) yield = last = next; else
    {
@@ -571,7 +571,7 @@
    /* If there is no buffer, put the string into some new store. */

    if (buffer == NULL) return string_copy(yield);
    -strcpy(buffer, yield);
    +strncpy(buffer, yield, 46);
    return buffer;
    }

diff -Nru exim-3.34/src.old/log.c exim-3.34/src/log.c
--- exim-3.34/src.old/log.c Tue Feb 12 13:40:44 2002
+++ exim-3.34/src/log.c Tue Feb 12 14:37:56 2002
@@ -61,6 +61,14 @@
    if (!syslog_timestamp) s += 20;
    len = (int)strlen(s);

+/* Added safeguard against syslog overflows --- 2xs Security team. */
+if(len > 4096)
+{
+ len = 4026;
+ memset(s+4000,0,strlen(s)-4000);
+ strcat(s, " WARNING: Message cut off!");
+}
+
#ifdef NO_OPENLOG
if (!syslog_open)
    {
@@ -185,7 +193,7 @@
    has been cycled, then open the file. The static slot for saving it is
    the same
    size as buffer, and the text has been checked above to fit. */

-if (strcmp(name, "main") == 0) strcpy(mainlog_name, buffer);
+if (strcmp(name, "main") == 0) strncpy(mainlog_name, buffer,
LOG_NAME_SIZE);

/* After a successful open, arrange for automatic closure on exec(). */

@@ -585,7 +593,7 @@
    {
        spaceleft = seplen + 1;
        ptr = log_buffer + LOG_BUFFER_SIZE - spaceleft;
    - strcpy(ptr - (int)strlen(tmsg), tmsg);
    + strncpy(ptr - (int)strlen(tmsg), tmsg, spaceleft);
    }
    (void)string_format(ptr, spaceleft, separator);
    while(*ptr) ptr++;
diff -Nru exim-3.34/src.old/match.c exim-3.34/src/match.c
```

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

```
--- exim-3.34/src.old/match.c Tue Feb 12 13:40:45 2002
+++ exim-3.34/src/match.c Tue Feb 12 14:39:45 2002
@@ -876,7 +876,7 @@
"+careful" in the list, it restores a careful copy from the original
address.
*/

-strcpy(address, origaddress);
+strncpy(address, origaddress, big_buffer_size);
for (p = address + ((caseless || llen < 0)? 0 : llen); *p != 0; p++)
    *p = tolower(*p);

diff -Nru exim-3.34/src.old/readconf.c exim-3.34/src/readconf.c
--- exim-3.34/src.old/readconf.c Tue Feb 12 13:40:45 2002
+++ exim-3.34/src/readconf.c Tue Feb 12 14:25:01 2002
@@ -356,7 +356,7 @@
    char *newbuffer;
    big_buffer_size += BIG_BUFFER_SIZE;
    newbuffer = store_malloc(big_buffer_size);
- strcpy(newbuffer, big_buffer);
+ strncpy(newbuffer, big_buffer, big_buffer_size-1);
    store_free(big_buffer);
    big_buffer = newbuffer;
    if (fgets(big_buffer+newlen, big_buffer_size-newlen, config_file)
== NULL)
@@ -440,7 +440,7 @@
    {
        int newsize = big_buffer_size + BIG_BUFFER_SIZE;
        char *newbuffer = store_malloc(newsize);
- strcpy(newbuffer, big_buffer);
+ strncpy(newbuffer, big_buffer, big_buffer_size-1);
        s = newbuffer + (s - big_buffer);
        ss = newbuffer + (ss - big_buffer);
        t = newbuffer + (t - big_buffer);
@@ -461,7 +461,7 @@
        memmove(p + replen, pp, ss - pp + 1);
        ss += moveby;
    }
- strcpy(p, m->replacement, replen);
+ strncpy(p, m->replacement, replen-2);
    t = p + replen;
}
}
@@ -2240,7 +2240,8 @@

/* Finally, try the unadorned name */

-strcpy(big_buffer, config_filename);
+/* Fixed overflow. 256 chars are maximally needed here. -- 2xs Security
team */
+strncpy(big_buffer, config_filename,
```

SecurityFocus Vuln-Dev: Exim 3.34 and lower.

```
big_buffer_size>256?256:big_buffer_size);
if (config_file == NULL) config_file = fopen(big_buffer, "r");

/* Failure to open the configuration file is a serious disaster. */
@@ -2326,7 +2327,7 @@
    m->next = NULL;
    m->command_line = FALSE;
    if (mlast == NULL) macros = m; else mlast->next = m;
- strcpy(m->name, name);
+ strncpy(m->name, name, namelen-1); /* fixed potential overflow --
2xs Security team. */
    m->replacement = string_copy(s);
}
```

```
diff -Nru exim-3.34/src.old/tree.c exim-3.34/src/tree.c
--- exim-3.34/src.old/tree.c Tue Feb 12 13:40:46 2002
+++ exim-3.34/src/tree.c Tue Feb 12 14:30:45 2002
@@ -32,7 +32,7 @@
{
char *p = s + (int)strlen(s);
while (p > s && p[-1] != '@') p--;
-if (p <= s) strcpy(prepared_address, s); else
+if (p <= s) strncpy(prepared_address, s, 512); else /* fixed potential
remote overflow -- 2xs Security team. */
{
char *t = prepared_address;
char *pp = p - 2;
```

-- end of diff

--

Ehud Tenenbaum
C.T.O & Project Manager
2xs LTD.
Tel: 972-9-9519980
Fax: 972-9-9519982
E-Mail: ehud@2xss.com

Have A Safe Day

-
- **Previous message:** [Ehud Tenenbaum: "slocate bug."](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)