

[UNIX] Metamail Format String and Buffer Overflows Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0056.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/19/04

To: list@securiteam.com

Date: 19 Feb 2004 12:35:39 +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>

Metamail Format String and Buffer Overflows Vulnerabilities

SUMMARY

" <<http://ftp.funet.fi/pub/unix/mail/metamail/>> Metamail is an implementation of MIME, the Multipurpose Internet Mail Extensions, a proposed standard for multimedia mail on the Internet. Metamail implements MIME, and also implements extensibility and configuration via the "mailcap" mechanism described in an informational RFC that is a companion to the MIME document".

There are several newsreaders (tin, slrn, nn), mailreaders (elm) and antivirus programs (antimime, older versions of AMaViS) that pass MIME messages from the network directly to metamail. Several vulnerabilities have been found in the product that would allow a remote attacker to cause the program to fail or execute arbitrary code (due to format string and buffer overflow vulnerabilities).

DETAILS

Vulnerable Systems:

* Metamail version 2.2, 2.4, 2.5, 2.6, 2.7

Securiteam: [UNIX] Metamail Format String and Buffer Overflows Vulnerabilities

Immune Systems:

* Metamail version 2.7 with the below patch

The first format string bug occurs when a message has a "multipart/alternative" media type and one of the body parts has a "Content-Type" header with parameter names or values containing formatting codes. It occurs because of two bad fprintf() statements in the function SaveSquirrelFile() in metamail.c. The file "testmail1" gives an example of this problem.

The second format string bug occurs when a message has encoded non-ASCII characters in the mail headers (as described in RFC 2047), an unknown encoding, and encoded text containing formatting codes. It is caused by a bad printf() statement in the function PrintHeader() in metamail.c. An example of this problem can be found in the file "testmail2".

The first buffer overflow occurs when a message has encoded non-ASCII characters in the mail headers and the part that names a character set is overly long. The root of this problem is a bad strcpy() statement in the function PrintHeader() in metamail.c. An example of this can be found in the file "testmail3".

The second buffer overflow doesn't occur in the metamail executable, but in the splitmail executable that's generated when you compile the metamail package. This overflow occurs when a message has an overly long Subject header. It is caused by a bad strcpy() statement in the function ShareThisHeader() in splitmail.c. An example can be found in the "testmail4.splitmail" file.

Patch and Test Messages:

Ulf has created metamail.advisory-data.tar.gz, which contains the four test messages mentioned above, as well as a patch that corrects all four issues (The patch is diff'ed against version 2.7), the file is available from: <http://labben.abm.uu.se/~ulha9485/metamail.advisory-data.tar.gz>

Disclosure Timeline:

As metamail is unmaintained, Ulf contacted the vendor-sec list instead.

7 feb: the vendor-sec list (vendor-sec@lst.de) was contacted

9 feb: a coordinated release date was agreed upon

Friday 13 feb (the day of the W2K source leak): CAN references were posted

18 feb: Slackware released their advisory and updates

18 feb: Ulf released this advisory

ADDITIONAL INFORMATION

The information has been provided by

<mailto:Ulf.Harnhammar.9485@student.uu.se> Ulf H?rnhammar.

=====

Securiteam: [UNIX] Metamail Format String and Buffer Overflows Vulnerabilities

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.