

possible open relay hole in qmail-smtpd-auth patch

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0176.html>

From: John Simpson (*jms1_at_jms1.net*)

Date: 07/15/03

To: smtpauth@list.elysium.pl, qmail@list.cr.yo.to, bugtraq@securityfocus.com

Date: Tue, 15 Jul 2003 12:36:05 -0400

the qmail-smtpd-auth patch is a commonly used patch to qmail which allows the qmail-smtpd program to support the AUTH extension, by specifying a "checkpassword" program on the command line. the homepage for the patch is:

<http://members.elysium.pl/brush/qmail-smtpd-auth/>

the patch modifies qmail-smtpd so that it can be called with three command-line parameters: the local host name (used for generating CRAM-MD5 challenges), the checkpassword program itself, and a "dummy" program which is run by the checkpassword program after a successful authentication.

the "dummy" program is needed because checkpassword programs are designed for use in a POP3 or IMAP situation, where they would validate the user's credentials and then run the actual POP3 or IMAP server program.

the current version of the SMTP-AUTH patch contains a serious bug which can accidentally allow somebody who forgets one or more of the command line parameters to start running an open relay by accident. it has been reported in several places over the last week, including this message on the qmail mailing list:

<http://marc.theaimsgroup.com/?l=qmail&m=105452174430616&w=2>

if the user forgets the hostname parameter to qmail-smtpd and uses /bin/true as the dummy program (/bin/true is the suggested dummy program), they will actually be using /bin/true as the checkpassword program, which allows ANY combination of userid and password to use your server as a relay.

i have written a revision to the qmail-smtpd-auth patch which compensates for this common error by not supporting the AUTH command unless all three command line arguments are present.

the version 0.31 patch does not correctly check for this- with a missing command line argument, it ends up reading memory beyond the end of argv[], which is NOT filled with zeros- on most *nix systems it's actually the

SecurityFocus Bugtraq: possible open relay hole in qmail-smtpd-auth patch

beginning of the environment block.

<http://www.jmsl.net/qmail/> has the modified "auth.patch" file available for download.

the changes i've made (actually CHECKING argc instead of assuming there will be something there) need to be incorporated into the qmail-smtpd-auth patch as soon as possible. the author of the patch seems to have not touched it since may 2002.

--

```
-----  
| John Simpson - KG4ZOW - Programmer At Large |  
| http://www.jmsl.net/ <jmsl@jmsl.net> |  
-----
```

-
- application/pgp-signature attachment: signature