CERT Advisory CA-1997-09 Vulnerability in IMAP and POP

Original issue date: April 7, 1997
Last revised: April 28, 1998
Added vendor information for Silicon Graphics Inc. Corrected URL for obtaining RFCs.

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of a vulnerability in some versions of the University of Washington's implementation of the Internet Message Access Protocol (IMAP) and Post Office Protocol (POP). Information about this vulnerability has been publicly distributed.

By exploiting this vulnerability, remote users can obtain unauthorized root access.

As of the August 4, 1997 update, intrusions based on the exploitation of this vulnerability continue to be reported to the CERT/CC.

The CERT/CC team recommends installing a patch if one is available or upgrading to IMAP4rev1. Until you can do so, we recommend disabling the IMAP and POP services at your site.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

The current version of Internet Message Access Protocol (IMAP) supports both online and offline operation, permitting manipulation of remote message folders. It provides access to multiple mailboxes (possibly on multiple servers), and supports nested mailboxes as well as resynchronization with the server. The current version also provides a user with the ability to create, delete, and rename mailboxes. Additional details concerning the functionality of IMAP can be found in RFC 2060 (the IMAP4rev1 specification) available from

ftp://ftp.isi.edu/in-notes/rfc2060.txt

The Post Office Protocol (POP) was designed to support offline mail processing. That is, the client connects to the server to download mail that the server is holding for the client. The mail is deleted from the server and is handled offline (locally) on the client machine.

In the implementation of both protocols on a UNIX system, the server must run with root privileges so it can access mail folders and undertake some file manipulation on behalf of the user logging in. After login, these privileges are discarded. However, in at least the University of Washington's implementation a vulnerability exists in the way the login transaction is handled. (See Appendix A for vendor information.) This vulnerability can be exploited to gain privileged access on the server. By preparing carefully crafted text to a system running a vulnerable version of these servers, remote users may be able to cause a buffer overflow and execute arbitrary instructions with root privileges.

Information about this vulnerability has been widely distributed.

II. Impact

Remote users can obtain root access on systems running a vulnerable IMAP or POP server. They do not need access to an account on the system to do this.

III. Solution

Install a patch from your vendor (see Section A) or upgrade to the latest version of IMAP (Section B). If your POP server is based on the University of Washington IMAP server code, you should also upgrade to the latest version of IMAP. Until you can take one of these actions, you should disable services (Section C). In all cases, we urge you to take the additional precaution described in Section D.

A. Obtain and install a patch from your vendor

Below is a list of vendors who have provided information about this vulnerability. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Carnegie Mellon University
Cray Research
Digital Equipment Corporation
IBM Corporation
Linux - Caldera, Inc.
Debian
Red Hat
Microsoft Corporation
NetManage, Inc.
Netscape
QUALCOMM, Incorporated
Silicon Graphics Inc.
Sun Microsystems, Inc.
University of Washington

B. Upgrade to the latest version of IMAP

An alternative to installing vendor patches is upgrading to IMAP4rev1, which is available from

ftp://ftp.cac.washington.edu/mail/imap.tar.Z

Please note that checksums change when files are updated. The imap.tar.Z file can undergo frequent changes, therefore the checksums have not been included here.

C. Disable services

Until you can take one of the above actions, temporarily disable the POP and IMAP services. On many systems, you will need to edit the /etc/inetd.conf file. However, you should check your vendor's documentation because systems vary in file location and the exact changes required (for example, sending the inetd process a HUP signal or killing and restarting the daemon).

If you are not able to temporarily disable the POP and IMAP services, then you should at least limit access to the vulnerable services to machines in your local network. This can be done by installing the tcp_wrappers described in Section D, not only for logging but also for access control. Note that even with access control via tcp_wrappers, you are still vulnerable to attacks from hosts that are allowed to connect to the vulnerable POP or IMAP service.

D. Additional precaution

Because IMAP or POP is launched out of inetd.conf, tcp_wrappers can be installed to log connections which can then be examined for suspicious activity. You may want to consider filtering connections at the firewall to discard unwanted/unauthorized connections.

The tcp_wrappers tool is available in

ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.5.tar.gz

MD5 (tcp_wrappers_7.5.tar.gz) = 8c7a17a12d9be746e0488f7f6bfa4abb

Note that this precaution does not address the vulnerability described in this advisory, but it is a good security practice in general.

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We're working on patches for both BSD/OS 2.1 and BSD/OS 3.0 for imap (which we include as part of pine).

Carnegie Mellon University

Cyrus Server 1.5.2, with full IMAP4rev1 and pop3 capabilities, is NOT affected by this report and is NOT vulnerable.

Cray Research

Not vulnerable.

Digital Equipment Corporation

This reported problem is not present for Digital's UNIX or Digital ULTRIX Operating Systems Software.

IBM Corporation

AIX 4.2.1 is the only version of AIX currently shipping with IMAP. Previous versions of AIX are not vulnerable.

AIX 4.2.1

The following APAR will be available soon:
APAR IX70263

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux Systems

Caldera, Inc.

On systems such as Caldera OpenLinux 1.0, an unprivileged user can obtain root access.

As a temporary workaround, you can disable the POP and IMAP services in /etc/inetd.conf, and then kill and restart inetd.

A better solution is to install the new RPM package that contains the fixed versions of the IMAP and POP daemons. They are located on Caldera's FTP server (ftp.caldera.com):

/pub/openlinux/updates/1.0/006/RPMS/imap-4.1.BETA-1.i386.rpm

The MD5 checksum (from the "md5sum" command) for this package is:

45a758dfd30f6d0291325894f9ec4c18

This and other Caldera security resources are located at:

http://www.caldera.com/tech-ref/security/

Debian

Debian linux is not vulnerable. For more information see

http://cgi.debian.org/www-master/debian.org/security.html

Red Hat

The IMAP servers included with all versions of Red Hat Linux have a buffer overrun which allow *remote* users to gain root access on systems which run them. A fix for Red Hat 4.1 is now available (details on it at the end of this note).

Users of Red Hat 4.0 should apply the Red Hat 4.1 fix. Users of previous releases of Red Hat Linux are strongly encouraged to upgrade or simply not run imap. You can remove imap from any machine running with Red Hat Linux 2.0 or later by running the command "rpm -e imap", rendering them immune to this problem.

All of the new packages are PGP signed with Red Hat's PGP key, and may be obtained from
ftp.redhat.com:/updates/4.1.

If you have direct Internet access, you may upgrade these packages on your system with the following commands:

Intel:
```
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/i386/imap-4.1.BETA-3.i386.rpm
MD5 (imap-4.1.BETA-3.i386.rpm) = 8ac64fff475ee43d409fc9776a6637a6
```

Alpha:
```
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/alpha/imap-4.1.BETA-3.alpha.rpm
MD5 (imap-4.1.BETA-3.alpha.rpm) = fd42ac24d7c4367ee51fd00e631cae5b
```

SPARC:
```
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/sparc/imap-4.1.BETA-3.sparc.rpm
MD5 (imap-4.1.BETA-3.sparc.rpm) = 751598aae3d179284b8ea4d7a9b78868
```

Microsoft

Microsoft's Exchange POP and IMAP servers and Microsoft's Commericial Internet System are not vulnerable

NetManage, Inc.

NetManage's ZPOP pop server is not vulnerable.

Netscape

Netscape's POP3/IMAP4 implementation is not vulnerable.

QUALCOMM Incorporated

Our engineers have examined the QPopper source code, which is based on source from UC Berkeley. They determined that QPopper is *NOT* vulnerable to a buffer overflow attack as described in CA-97.09. It strictly checks the size of messages before copying them into its buffer.

Silicon Graphics Inc.

Silicon Graphics Inc. Security Advisory, 19980302-01-I, provides the following information:

The Internet Mail Access Protocol (IMAP) & Post Office Protocol (POP) provide users with an alternative means to process and retrieve their email.

A vulnerability has been discovered in IMAP4 & POP3 that allows remote users to obtain root access.

Silicon Graphics sells and supports the Netscape Mail/Messaging Servers for IRIX which use IMAP4 & POP3 however, their implementations are not vulnerable to this issue and no further action is required.

More information about Netscape product security can be found at the following URL:

http://home.netscape.com/assist/security/

Sun Microsystems, Inc.

The following patches have been released for CERT CA-97.09.

> *105346-02 SIMS 2.0*
> *105347-02 SIMS 2.0_x86*

University of Washington

This vulnerability has been detected in the University of Washington c-client library used in the UW IMAP and POP servers. This vulnerability affects all versions of imapd prior to v10.165, all versions of ipop2d prior to 2.3(32), and all versions of ipop3d prior to 3.3(27).

It is recommended that all sites using these servers upgrade to the latest versions, available in the UW IMAP toolkit:

ftp://ftp.cac.washington.edu/mail/imap.tar.Z

Please note that checksums change when files are updated. The imap.tar.Z file can undergo frequent changes, therefore the checksums have not been included here.

This is a source distribution which includes imapd, ipop2d, ipop3d. and the c-client library. The IMAP server in this distribution conforms with RFC2060 (the IMAP4rev1 specification).

Sites which are not yet prepared to upgrade from IMAP2bis to IMAP4 service may obtain a corrected IMAP2bis server as part of the latest (3.96) UW Pine distribution, available at:

ftp://ftp.cac.washington.edu/pine/pine.tar.Z

MD5 (pine.tar.Z) = 37138f0d1ec3175cf1ffe6c062c9abbf

The CERT Coordination Center thanks the University of Washington's Computing and Communications staff for information relating to this advisory. We also thank Wolfgang Ley of DFN-CERT for his input. We thank Matthew Wall of Carnegie Mellon University for additional insightful feedback.

UPDATES

April 8, 1997

We have received requests for clarification. The vulnerability described in this advisory relates to certain server implementations and is not in the protocol itself. See Appendix A for vendor and server information.

Revision History

```
Apr. 28. 1998 Added vendor information for Silicon Graphics Inc.
              Corrected URL for obtaining RFCs.
Jan. 15, 1998 Updated vendor information for Sun Microsystems, Inc.
Sep. 26, 1997 Updated copyright statment
Aug. 27, 1997 Section III.A and Appendix A - added vendor information for
              IBM Corporation.
Aug 4, 1997   Clarifications in wording have been made to the introduction and
              paragraph 3 of the description section.
June 3, 1997  Section III.A and Appendix - Added vendor information for NetManage, Inc.
May 1, 1997   Section III.A and Appendix A - Added vendor information for
              Microsoft Corporation.
Apr 18, 1997  Section III.A and Appendix A - Added vendor information for
              Debian and Netscape.
Apr 11, 1997  Section III.B. - Removed checksum information for the imap.tar.Z
              distribution and added an explanation.
Apr 9, 1997   Appendix A - added vendor information for Digital
              Equipment Corporation and QUALCOMM Incorporated.
              Updated vendor information for Sun Microsystems,
              Inc. Added another name to acknowledgment.
Apr 08, 1997  Updates - Added clarification that the vulnerability is
              an implementation error and not an error in the protocol
              Appendix - added vendor information for Caldera and the
              Carnegie Mellon University Cyrus Server
              Acknowledgments - Added a name that was inadvertently left out.
```