CERT Advisory CA-2003-07 Remote Buffer Overflow in Sendmail

Original release date: March 3, 2003
Last revised: June 09, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sendmail Pro (all versions)
- Sendmail Switch 2.1 prior to 2.1.5
- Sendmail Switch 2.2 prior to 2.2.5
- Sendmail Switch 3.0 prior to 3.0.3
- Sendmail for NT 2.X prior to 2.6.2
- Sendmail for NT 3.0 prior to 3.0.3
- Systems running open-source sendmail versions prior to 8.12.8, including UNIX and Linux systems

Overview

There is a vulnerability in sendmail that may allow remote attackers to gain the privileges of the sendmail daemon, typically root.

I. Description

Researchers at Internet Security Systems (ISS) have discovered a remotely exploitable vulnerability in sendmail. This vulnerability could allow an intruder to gain control of a vulnerable sendmail server.

Most organizations have a variety of mail transfer agents (MTAs) at various locations within their network, with at least one exposed to the Internet. Since sendmail is the most popular MTA, most medium-sized to large organizations are likely to have at least one vulnerable sendmail server. In addition, many UNIX and Linux workstations provide a sendmail implementation that is enabled and running by default.

This vulnerability is message-oriented as opposed to connection-oriented. That means that the vulnerability is triggered by the contents of a specially-crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability will pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through many common packet filters or firewalls.

Sendmail has indicated to the CERT/CC that this vulnerability has been successfully exploited in a laboratory environment. We do not believe that this exploit is available to the public. However, this vulnerability is likely to draw significant attention from the intruder community, so the probability of a public exploit is high.

A successful attack against an unpatched sendmail system will not leave any messages in the system log. However, on a patched system, an attempt to exploit this vulnerability will leave the following log message:

> *Dropped invalid comments from header address*

Although this does not represent conclusive evidence of an attack, it may be useful as an indicator.

A patched sendmail server will drop invalid headers, thus preventing downstream servers from receiving them.

The CERT/CC is tracking this issue as VU#398025. This reference number corresponds to CVE candidate CAN-2002-1337.

For more information, please see

http://www.sendmail.org
http://www.sendmail.org/8.12.8.html
http://www.sendmail.com/security/
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950
http://www.kb.cert.org/vuls/id/398025

II. Impact

Successful exploitation of this vulnerability may allow an attacker to gain the privileges of the sendmail daemon, typically root. Even vulnerable sendmail servers on the interior of a given network may be at risk since the vulnerability is triggered from the contents of a malicious email message.

III. Solution

Apply a patch from Sendmail

Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12. However, the vulnerability also exists in earlier versions of the code; therefore, site administrators using an earlier version are encouraged to upgrade to 8.12.8. These patches are located at

ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.security.cr.patch
ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.11.6.security.cr.patch
ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.9.3.security.cr.patch

Apply a patch from your vendor

Many vendors include vulnerable sendmail servers as part of their software distributions. We have notified vendors of this vulnerability and recorded their responses in the systems affected section of VU#398025. Several vendors have provided a statement for direct inclusion in this advisory; these statements are available in Appendix A.

Enable the RunAsUser option

There is no known workaround for this vulnerability. Until a patch can be applied, you may wish to set the RunAsUser option to reduce the impact of this vulnerability. As a good general practice, the CERT/CC recommends limiting the privileges of an application or service whenever possible.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Security Update 2003-03-03 is available to fix this issue. Packages are available for Mac OS X 10.1.5 and Mac OS X 10.2.4. It should be noted that sendmail is not enabled by default on Mac OS X, so only those systems which have explicitly enabled it are susceptible to the vulnerability. All customers of Mac OS X, however, are encouraged to apply this update to their systems.

Avaya, Inc.

Avaya is aware of the vulnerability and is investigating impact. As new information is available this statement will be updated.

BSD/OS

Wind River Systems has created patches for this problem which are available from the normal locations for each release. The relevant patches are M500-006 for BSD/OS version 5.0 or the Wind River Platform for Server Appliances 1.0, M431-002 for BSD/OS 4.3.1, or M420-032 for BSD /OS 4.2 systems.

Cisco Systems

Cisco is investigating this issue. If we determine any of our products are vulnerable that information will be available at: http://www.cisco.com/go /psirt

Cray Inc.

The code supplied by Cray, Inc. in Unicos, Unicos/mk, and Unicos/mp may be vulnerable. Cray has opened SPRs 724749 and 724750 to investigate.

Cray, Inc. is not vulnerable for the MTA systems.

Debian

Updated packages for sendmail and sendmail-wide will be available at http://www.debian.org/security/2003/dsa-257

Hewlett-Packard Company

```
SOURCE:
         Hewlett-Packard Company
         HP Services
         Software Security Response Team

x-ref: SSRT3469

  HP released security bulletins for this issue on 03 March 2003
  and recently updated 11 March 2003 for Internet Express and
  AVFW98.

  View at www.hp.com  and in the search window type SSRT3469

  For HP-UX use your normal ITRC access and select Security
  Bulletin HPSBUX0302-246


    This problem affects supported versions of HP-UX,
    HP Tru64 UNIX/TruCluster Server,
    HP AlphaServer SC (Sierra Cluster) V2.5,
    HP Internet Express,
    HP AltaVista Firewall (AVFW98 / Raptor EC).


    NOTE: This problem does not impact
                HP NonStop Servers nor  HP OpenVMS.
```

Hitachi, Ltd.

```
Hitachi's GR2000 gigabit router series
  - is NOT vulnerable, because it does not support sendmail.

Hitachi's HI-UX/WE2
  - is NOT vulnerable.

If you need technical information, please contact Hitachi's support.
```

IBM Corporation

The AIX operating system is vulnerable to the sendmail issues discussed in releases 4.3.3, 5.1.0 and 5.2.0.

IBM provides the following official fixes:

APAR number for AIX 4.3.3: IY40500
APAR number for AIX 5.1.0: IY40501
APAR number for AIX 5.2.0: IY40502

Please contact your local IBM AIX support center for any assistance.

Juniper Networks

Sendmail does not ship with any Juniper Networks product, so there is no vulnerability to this issue.

Lotus

IBM has determined that Lotus products, including Notes and Domino, are not vulnerable to the sendmail issues reported by ISS.

MandrakeSoft

MandrakeSoft has issued updated sendmail packages that are not vulnerable to this problem by using the patches provided by the sendmail development team. Users can use urpmi or the Software Manager to upgrade packages. The web advisory is available: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:028

Nortel Networks

The following Nortel Networks Wireless products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-07:

SS7 IP Gateway. Nortel Networks recommends disabling Sendmail as it is not used.
Wireless Preside OAM&P Main Server. Sendmail should not be disabled on these products.

The following Nortel Networks Enterprise Voice IVR products are potentially affected by the vulnerabilities identified in CERT Advisory CA-2003-07:

MPS1000
MPS500
VPS

CTX

All the above products deploy Sendmail; it should not be disabled on these products.

For all of the above products Nortel Networks recommends applying the latest Sun Microsystems patches in accordance with that vendor's recommendations. To avoid applying patches twice, please ensure that the Sun Microsystems patch applied also addresses the vulnerability identified in CERT Advisory CA-2003-12.

The following Nortel Networks Succession products are potentially affected by the vulnerability identified in CERT Advisory CA-2003-07:

SSPFS-based CS2000 Management Tools
GWC Element Manager and QoS Collector Application (QCA)
SAM21 Element Manager
Audio Provisioning Server (APS) and APS client GUI
UAS Element Manager
Succession Media Gateway 9000 Element Manager (Mid-Tier and Server)
Network Patch Manager (NPM)
Nodes Configuration, Trunk Configuration, Carrier Endpoint Configuration, Lines Configuration (Servord+), Trunk Maintenance Manager, Lines Maintenance Manager, Line Test Manager, V5.2 Configuration and Maintenance, PM Poller, EMS Proxy Services, and Common Application Launch Point
A product bulletin will be issued shortly.

Sendmail has been disabled in SN06 and therefore SN06 is not vulnerable. A patch for SN05 is currently under development that will disable Sendmail in SN05 so that it will not be affected by the vulnerability identified in CERT Advisory CA-2003-07. The availability date for the SN05 patch is still to be determined.

For more information please contact Nortel at:

North America: 1-800-4NORTEL or 1-800-466-7835
Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009
Contacts for other regions are available at http://www.nortelnetworks.com/help/contact/global/

Openwall GNU/*/Linux

Openwall GNU/*/Linux is not vulnerable. We use Postfix as the MTA, not sendmail.

Postfix

Postfix 2.0.6 duplicates the Sendmail 8.12.8 fix to in order to help protect downstream Sendmail systems against exploitation of this vulnerability. Patches are also available for several older Postfix releases. For download information, please see http://www.postfix.org/.

Red Hat Inc.

Updated sendmail packages that are not vulnerable to this issue are available for Red Hat Linux, Red Hat Advanced Server, and Red Hat Advanced Workstation. Red Hat Network users can update their systems using the 'up2date' tool.

Red Hat Linux:

> *http://rhn.redhat.com/errata/RHSA-2003-073.html*

Red Hat Linux Advanced Server, Advanced Workstation:

> *http://rhn.redhat.com/errata/RHSA-2003-074.html*

Sequent Computer Systems (IBM)

For information please contact IBM Service at 1-800-IBM-SERV.

SGI

SGI acknowledges VU#398025 reported by CERT and has released an advisory to address the vulnerability on IRIX.

Refer to SGI Security Advisory 20030301-01-P available from ftp://patches.sgi.com/support/free/security/advisories/20030301-01-P or http://www.sgi.com/support/security/.

The Sendmail Consortium

The Sendmail Consortium suggests that sites upgrade to 8.12.8 if possible. Alternatively, patches are available for 8.9, 8.10, 8.11, and 8.12 on http://www.sendmail.org/

Sendmail, Inc.

All commercial releases including Sendmail Switch, Sendmail Advanced Message Server (which includes the Sendmail Switch MTA), Sendmail for NT, and Sendmail Pro are affected by this issue. Patch information is available at http://www.sendmail.com/security.

Sun Microsystems

Solaris 2.6, 7, 8 and 9 are vulnerable to VU#398025.

Sun will be publishing a Sun Alert for the issue at the following location shortly:

> *http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/51181*

The patches listed in the Sun Alert will be available from:

> *http://sunsolve.sun.com/securitypatch*

Syntegra

None of Syntegra's mail products, including IntraStore, eMail Sentinel and Mail*Hub are vulnerable to this defect.

Xerox Corporation

A response to this advisory is available from our web site: http://www.xerox.com/security.

Our thanks to Internet Security Systems, Inc. for discovering this problem, and to Eric Allman, Claus Assmann, and Greg Shapiro of Sendmail for notifying us of this problem. We thank both groups for their assistance in coordinating the response to this problem.

Authors: Jeffrey P. Lanza and Shawn V. Hernan

Revision History

```
Mar 03, 2003:  Initial release
Mar 03, 2003:  Added statement for Sun Microsystems
Mar 03, 2003:  Fixed typo in mailto: URL
Mar 04, 2003:  Added statements for Juniper Networks, MandrakeSoft, and Hitachi
Mar 04, 2003:  Added statement for Debian
Mar 04, 2003:  Added statement for Lotus
Mar 10, 2003:  Added statement for Postfix
Mar 12, 2003:  Updated statement for Hewlett-Packard
Mar 13, 2003:  Updated statement for IBM
Mar 27, 2003:  Updated statement for Hitachi
Apr 22, 2003:  Added statement for Nortel Networks; statement submitted on 8-Apr-2003
Jun 09, 2003:  Added statements for Sequent, Syntegra, and Xerox
```