

FreeBSD Security Advisory FreeBSD–SA–01:

Source: <http://www.derkeiler.com/Mailing–Lists/FreeBSD–Security/2001–04/2600.html>

From: FreeBSD Security Advisories (security–advisories@FreeBSD.org)

Date: 04/24/01

Date: Mon, 23 Apr 2001 20:17:03 –0700 (PDT)

From: FreeBSD Security Advisories <security–advisories@FreeBSD.org>

To: FreeBSD Security Advisories <security–advisories@FreeBSD.org>

-----BEGIN PGP SIGNED MESSAGE-----

=====

FreeBSD–SA–01:34 Security Advisory

FreeBSD, Inc.

Topic: hylafax contains local compromise

Category: ports

Module: hylafax

Announced: 2001–04–23

Credits: Marcin Dawcewicz <miv@IIDEA.PL>

Affects: Ports collection prior to the correction date.

Corrected: 2001–04–17

Vendor status: Updated version released

FreeBSD only: NO

I. Background

HylaFAX is a facsimile system for UNIX systems.

II. Problem Description

The hylafax port, versions prior to hylafax–4.1.b2_2, contains a format string bug in the hfaxd program. A local user may execute the hfaxd program with command–line arguments containing format string characters, potentially gaining root privileges on the local system.

The hylafax port is not installed by default, nor is it "part of FreeBSD" as such: it is part of the FreeBSD ports collection, which contains over 5000 third–party applications in a ready–to–install format. The ports collections shipped with FreeBSD 3.5.1 and 4.2 contain this problem since it was discovered after the releases.

The ports collection that shipped with FreeBSD 4.3 is not vulnerable since this problem was corrected prior to the release.

FreeBSD–Security: FreeBSD Security Advisory FreeBSD–SA–01:

FreeBSD makes no claim about the security of these third–party applications, although an effort is underway to provide a security audit of the most security–critical ports.

III. Impact

Local users may gain root privileges on the local system.

If you have not chosen to install the hylafax port/package, then your system is not vulnerable to this problem.

IV. Workaround

Deinstall the hylafax port/package if you have installed it.

V. Solution

One of the following:

- 1) Upgrade your entire ports collection and rebuild the hylafax port.
- 2) Deinstall the old package and install a new package dated after the correction date, obtained from:

[i386]

ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/comms/hylafax-4.1.b2_2.tgz
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-5-current/comms/hylafax-4.1.b2_2.tgz

NOTE: it may be several days before updated packages are available.

[alpha]

Packages are not automatically generated for the alpha architecture at this time due to lack of build resources.

- 3) download a new port skeleton for the hylafax port from:

<http://www.freebsd.org/ports/>

and use it to rebuild the port.

- 4) Use the portcheckout utility to automate option (3) above. The portcheckout port is available in /usr/ports/devel/portcheckout or the package can be obtained from:

<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-3-stable/devel/portcheckout-2.0.tgz>
<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/devel/portcheckout-2.0.tgz>
<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/alpha/packages-4-stable/devel/portcheckout-2.0.tgz>
<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-5-current/devel/portcheckout-2.0.tgz>
<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/alpha/packages-5-current/devel/portcheckout-2.0.tgz>

FreeBSD–Security: FreeBSD Security Advisory FreeBSD–SA–01:

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.4 (FreeBSD)

Comment: FreeBSD: The Power To Serve

iQCVAwUBOuTqs1UuHi5z0oilAQEWwgQAlhOueE800ddI0J9hiGsQKli2LJyQ18ObQ
w0/rdjahJDkOLrx5IGlFe9M1IzjbeXauYT6TUnaOxfwMo58bUy1T7QZ9ROUYzE39
DzrN1JmjcTshG3HdgsdVfSwjQirYpN6uvRVWQx6ncMpuN5bSw3RZ3ci4WH/LsKty
tZ9P/gD6bAs=
=EFP3

-----END PGP SIGNATURE-----

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message