

[UNIX] HylaFAX Format String Vulnerability (Fixed)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/12/03

To: list@securiteam.com

Date: 12 Nov 2003 20:24:59 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

HylaFAX Format String Vulnerability (Fixed)

SUMMARY

<<http://www.hylafax.org>> HylaFAX is "a mature (est. 1991) enterprise-class open source software package for sending and receiving facsimiles as well as for sending alpha-numeric pages. It runs on a wide variety of UNIX-like platforms including Linux, BSD (including Mac OS X), SunOS and Solaris, SCO, IRIX, AIX, and HP-UX".

The SuSE Security Team recently audited the HylaFAX daemon (hfaxd) and discovered a remotely exploitable format string vulnerability.

A vulnerable host must have set the 0x002 bit for the ServerTracing configuration parameter. This is not the default setting for the HylaFAX installation, but it is not an uncommon configuration when troubleshooting HylaFAX operation.

DETAILS

Vulnerable systems:

- * HylaFAX version 4.1.7 and prior

Immune systems:

- * HylaFAX version 4.1.8

Securiteam: [UNIX] HylaFAX Format String Vulnerability (Fixed)

Solution:

HylaFAX development has released the 4.1.8 patch-level code release which includes the fix for this format string vulnerability as contributed by SuSE. All users are strongly encouraged to upgrade.

Availability:

HylaFAX 4.1.8 is available by anonymous ftp at:
<<ftp://ftp.hylafax.org/source/hylafax-4.1.8.tar.gz>>
<ftp://ftp.hylafax.org/source/hylafax-4.1.8.tar.gz>.
(Binary versions will shortly be made available)

The fix is available in patch form at:

<http://bugs.hylafax.org/bugzilla/show_bug.cgi?id=468>
http://bugs.hylafax.org/bugzilla/show_bug.cgi?id=468.

There is no known exploitation in the wild of this vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lee.howard@hylafax.org>> Lee Howard.

=====

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.