FreeBSD 5.4-RELEASE Errata

The FreeBSD Project

$FreeBSD: src/release/doc/en_US.ISO8859-1/errata/article.sgml,v 1.69.2.22 2005/06/13 17:13:23 hrs Exp $

This document lists errata items for FreeBSD 5.4-RELEASE, containing significant information discovered after the release or too late in the release cycle to be otherwise included in the release documentation. This information includes security advisories, as well as news relating to the software or documentation that could affect its operation or usability. An up-to-date version of this document should always be consulted before installing this version of FreeBSD.

This errata document for FreeBSD 5.4-RELEASE will be maintained until the release of FreeBSD 5.5-RELEASE.

1 Introduction

This errata document contains "late-breaking news" about FreeBSD 5.4-RELEASE. Before installing this version, it is important to consult this document to learn about any post-release discoveries or problems that may already have been found and fixed.

Any version of this errata document actually distributed with the release (for example, on a CDROM distribution) will be out of date by definition, but other copies are kept updated on the Internet and should be consulted as the "current errata" for this release. These other copies of the errata are located at http://www.FreeBSD.org/releases/, plus any sites which keep up-to-date mirrors of this location.

Source and binary snapshots of FreeBSD 5-STABLE also contain up-to-date copies of this document (as of the time of the snapshot).

For a list of all FreeBSD CERT security advisories, see http://www.FreeBSD.org/security/ or ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/.

2 Security Advisories

The following security advisories pertain to FreeBSD 5.4-RELEASE. For more information, consult the individual advisories available from ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/.

Advisory	Date	Topic
SA-05:09.htt[a]	22 May 2005	information disclosure when using HTT
SA-05:10.tcpdump[b]	9 Jun 2005	Infinite loops in tcpdump protocol decoding
SA-05:11.gzip[c]	9 Jun 2005	gzip directory traversal and permission race vulnerabilities
SA-05:12.bind9[d]	9 Jun 2005	BIND 9 DNSSEC remote denial of service vulnerability

a. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:09.htt.asc

b. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:10.tcpdump.asc

c. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:11.gzip.asc

d. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:12.bind9.asc

3 Open Issues

No issues.

4 Late-Breaking News

(6 May 2005) An error in the default permissions on the `/dev/iir` device node, which allowed unprivileged local users to send commands to the hardware supported by the iir(4) driver. Although the error was fixed prior to 5.4-RELEASE, it was applied too late in the release cycle to be mentioned in the release notes. For more information, see security advisory FreeBSD-SA-05:06.iir[1].

(6 May 2005) A bug in the validation of i386_get_ldt(2) system call input arguments, which may allow kernel memory may be disclosed to the user process, has been fixed. This bug was fixed prior to 5.4-RELEASE, although not in time to be mentioned in the release notes. For more information, see security advisory FreeBSD-SA-05:07.ldt[2].

(6 May 2005) Several information disclosure vulnerabilities in various parts of the kernel have been fixed in 5.4-RELEASE, although too late to be mentioned in the release notes. For more information, see security advisory FreeBSD-SA-05:08.kmem[3].

1. ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:06.iir.asc
2. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:07.ldt.asc
3. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:08.kmem.asc