FreeBSD Security Information

Introduction

FreeBSD takes security very seriously and its developers are constantly working on making the operating system as secure as possible. This page will provide information about what to do in the event of a security vulnerability affecting your system.

Table of Contents

Reporting FreeBSD security incidents

FreeBSD security issues specific to the base system should be reported via email to the FreeBSD Security Team or, if a higher level of confidentiality is required, via PGP encrypted email to the Security Officer Team using the Security Officer PGP key. Additional information can be found at the reporting FreeBSD security incidents page.

When is a Security Advisory considered?

For every issue that gets reported, an internal tracking number is created, unless something is very obviously not a security issue. To determine whether or not a Security Advisory is warranted we use the following scheme:

- Is it a privilege escalation vulnerability?
- Is it a code injection vulnerability?
- Is it a memory disclosure or dataleak vulnerability?
  - From either the kernel
  - From a privileged process
  - From a process owned by another user?
- Is it a Denial of Service vulnerability?
  - Only when remotely exploitable, where remotely means that it comes from a different broadcast domain, so ARP and/or NDP based attacks do not qualify.
- Is it an unassisted jailbreak vulnerability?
- Is it a malfunction that could lead to generating insecure crypto keys, such as a PRNG bug?

For items that fall under these categories, a Security Advisory is very likely. Items that are not on this list are looked into individually and it will be determined then whether or not it will receive a Security Advisory or an Errata Notice.

Once it had been determined that a Security Advisory is warranted, either the submitter delivers a CVE number if he/she already requested one, or we use one from the FreeBSD pool available.

Recent FreeBSD security vulnerabilities

A full list of all security vulnerabilities affecting the base system can be found on this page.

A full list of all other errata affecting the base system can be found on this page.

Understanding FreeBSD security advisories

Advisories affecting the base system are sent to the following mailing lists:

- FreeBSD-security-notifications@FreeBSD.org
- FreeBSD-security@FreeBSD.org
- FreeBSD-announce@FreeBSD.org

The list of released advisories can be found on the FreeBSD Security Advisories page.

Advisories are always signed using the FreeBSD Security Officer PGP key and are archived, along with their associated patches, at the https://security.FreeBSD.org web server in the advisories and patches subdirectories.

The FreeBSD Security Officer provides security advisories for *-STABLE Branches* and the *Security Branches*. (Advisories are not issued for the *-CURRENT Branch*, which is primarily oriented towards FreeBSD developers.)

- The -STABLE branch tags have names like `stable/13`. The corresponding builds have names like `FreeBSD 13.3-STABLE`.
- Each FreeBSD Release has an associated Security Branch. The Security Branch tags have names like `releng/13.3`. The corresponding builds have names like `FreeBSD 13.3-RELEASE-p1`.

Issues affecting the FreeBSD Ports Collection are covered separately in the FreeBSD VuXML document.

Errata affecting the base system but not classified as security vulnerabilities are covered separately on the FreeBSD Errata Notices page.

How to update your system

If you have previously installed a binary version of FreeBSD (e.g., 13.2 or 14.0), run two commands:

```
# freebsd-update fetch
```

```
# freebsd-update install
```

If that fails, follow the other instructions in the security advisory you care about.

Note that the above procedure is only for users who have previously installed a binary distribution. Those who have built from source will need to update their source tree to upgrade.

For more details, read how to apply security patches.

Supported FreeBSD releases

Each release is supported by the Security Officer for a limited time only.

The designation and expected lifetime of all currently supported branches and their respective releases are given below. The *Expected EoL (end-of-life)* column indicates the earliest date on which support for that branch or release will end. Please note that these dates may be pushed back if circumstances warrant it.

Older releases are not supported and users are strongly encouraged to upgrade to one of these supported releases:

Branch	Release	Release Date	Expected EoL
stable/14	n/a	n/a	November 30, 2028
releng/14.0	14.0-RELEASE	November 20, 2023	14.1-RELEASE + 3 months
stable/13	n/a	n/a	January 31, 2026
releng/13.2	13.2-RELEASE	April 11, 2023	June 30, 2024
releng/13.3	13.3-RELEASE	March 5, 2024	13.4-RELEASE + 3 months

In the run-up to a release, a number of -BETA and -RC releases may be published for testing purposes. These releases are only supported for a few weeks, as resources permit, and will not be listed as supported on this page. Users are strongly discouraged from running these releases on production systems.

The FreeBSD support model

Under the current support model, each major version’s stable branch is explicitly supported for 5 years, while each individual point release is only supported for three months after the next point release.

The details and rationale behind this model can be found in the official announcement sent in February 2015.

Last modified on: March 10, 2024 by Graham Perrin