Debian security FAQ

Q: I received a DSA via debian-security-announce, how can I upgrade the vulnerable packages?

A: As the DSA mail says, you should upgrade the packages affected by the announced vulnerability. You can do this by just upgrading (after updating the list of available packages with `apt-get update`) every package in your system with `apt-get upgrade` or by upgrading just a particular package, with `apt-get install package`.

The announcement mail mentions the source package in which the vulnerability was present. Therefore, you should update all the binary packages from that source package. To check the binary packages to update, visit `https://packages.debian.org/src:source-package-name` and click on *[show ... binary packages]* for the distribution you are updating.

It may also be necessary to restart a service or a running process. The command `checkrestart` included in the package debian-goodies might help to find which ones.

Q: The signature on your advisories does not verify correctly!

A: This is most likely a problem on your end. The debian-security-announce list has a filter that only allows messages with a correct signature from one of the security team members to be posted.

Most likely some piece of mail software on your end slightly changes the message that breaks the signature. Make sure your software does not do any MIME encoding or decoding, or tab/space conversions.

Known culprits are fetchmail (with the mimedecode option enabled), formail (from procmail 3.14 only) and evolution.

Q: How is security handled in Debian?

A: Once the security team receives a notification of an incident, one or more members review it and consider its impact on the stable release of Debian (i.e. if it's vulnerable or not). If our system is vulnerable, we work on a fix for the problem. The package maintainer is contacted as well, if they didn't contact the security team already. Finally, the fix is tested and new packages are prepared, which are then compiled on all stable architectures and uploaded afterwards. After all of that is done, an advisory is published.

Q: Why are you fiddling with an old version of that package?

The most important guideline when making a new package that fixes a security problem is to make as few changes as possible. Our users and developers are relying on the exact behaviour of a release once it is made, so any change we make can possibly break someone's system. This is especially true in case of libraries: make sure you never change the Application Program Interface (API) or Application Binary Interface (ABI), no matter how small the change is.

This means that moving to a new upstream version is not a good solution, instead the relevant changes should be backported. Generally upstream maintainers are willing to help if needed, if not the Debian security team might be able to help.

In some cases it is not possible to backport a security fix, for example when large amounts of source code need to be modified or rewritten. If that happens it might be necessary to move to a new upstream version, but this has to be coordinated with the security team beforehand.

Q: The version number for a package indicates that I am still running a vulnerable version!

A: Instead of upgrading to a new release we backport security fixes to the version that was shipped in the stable release. The reason we do this is to make sure that a release changes as little as possible so things will not change or break unexpectedly as a result of a security fix. You can check if you are running a secure version of a package by looking at the package changelog, or comparing its exact version number with the version indicated in the Debian Security Advisory.

Q: I received an advisory, but the build for one processor architecture seems to be missing.

A: Generally the Security Team releases an advisory with builds of the updated packages for all architectures that Debian supports. However, some architectures are slower than others and it may happen that builds for most architectures are ready while some are still missing. These smaller archs represent a small fraction of our user base. Depending on the urgency of the issue we may decide to release the advisory forthwith. The missing builds will be installed as soon as they come available, but no further notice of this will be given. Of course we will never release an advisory where the i386 or amd64 builds are not present.

Q: How is security handled for `unstable`?

A: Security for unstable is primarily handled by package maintainers, not by the Debian Security Team. Although the security team may upload high-urgency security-only fixes when maintainers are noticed to be inactive, support for stable will always have priority. If you want to have a secure (and stable) server you are strongly encouraged to stay with stable.

Q: How is security handled for `testing`?

A: Security for testing benefits from the security efforts of the entire project for unstable. However, there is a minimum two-day migration delay, and sometimes security fixes can be held up by transitions. The Security Team helps to move along those transitions holding back important security uploads, but this is not always possible and delays may occur. Especially in the months after a new stable release, when many new versions are uploaded to unstable, security fixes for testing may lag behind. If you want to have a secure (and stable) server you are strongly encouraged to stay with stable.

Q: How is security handled for `contrib` and `non-free`?

A: The short answer is: it's not. Contrib and non-free aren't official parts of the Debian Distribution and are not released, and thus not supported by the security team. Some non-free packages are distributed without source or without a license allowing the distribution of modified versions. In those cases no security fixes can be made at all. If it is possible to fix the problem, and the package maintainer or someone else provides correct updated packages, then the security team will generally process them and release an advisory.

Q: The advisory says unstable is fixed in version 1.2.3-1, but unstable has 1.2.5-1, what's up?

A: We try to list the first version in unstable that fixed the problem. Sometimes the maintainer has uploaded even newer versions in the meantime. Compare the version in unstable with the version we indicate. If it's the same or higher, you should be safe from this vulnerability. If you want to be sure, you can check the package changelog with `apt-get changelog package-name` and search for the entry announcing the fix.

Q: Why are there no official mirrors for security.debian.org?

A: Actually, there are. There are several official mirrors, implemented through DNS aliases. The purpose of security.debian.org is to make security updates available as quickly and easily as possible.

Encouraging the use of unofficial mirrors would add extra complexity that is usually not needed and that can cause frustration if these mirrors are not kept up to date.

Q: I've seen DSA 100 and DSA 102, now where is DSA 101?

A: Several vendors (mostly of GNU/Linux, but also of BSD derivatives) coordinate security advisories for some incidents and agree to a particular timeline so that all vendors are able to release an advisory at the same time. This was decided in order to not discriminate some vendors that need more time (e.g. when the vendor has to pass packages through lengthy QA tests or has to support several architectures or binary distributions). Our own security team also prepares advisories in advance. Every now and then, other security issues have to be dealt with before the parked advisory could be released, and hence temporarily leaving out one or more advisories by number.

Q: How can I reach the security team?

A: Security information can be sent to security@debian.org or team@security.debian.org, both of which are read by the members of the security team.

If desired, email can be encrypted with the Debian Security Contact key (key ID 0x0D59D2B15144766A14D241C66BAF400B05C3E651). For the PGP/GPG keys of individual team members, please refer to the keyring.debian.org keyserver.

Q: I guess I found a security problem, what should I do?

A: If you learn about a security problem, either in one of your own packages or in someone else's please always contact the security team. If the Debian security team confirms the vulnerability and other vendors are likely to be vulnerable as well, they usually contact other vendors as well. If the vulnerability is not yet public they will try to coordinate security advisories with the other vendors, so all major distributions are in sync.

If the vulnerability is already publicly known, be sure to file a bug report in the Debian BTS, and tag it *“security”*.

If you are a Debian maintainer, see below.

Q: What am I supposed to do with a security problem in one of my packages?

A: If you learn of a security problem, either in your package or someone else's please always contact the security team via email at team@security.debian.org. They keep track of outstanding security problems, can help maintainers with security problems or fix problems on their own, are responsible for sending out security advisories and maintaining security.debian.org.

The Developer's Reference has complete instructions on what to do.

It's particularly important that you don't upload to any other distribution other than unstable without prior agreement by the security team, because bypassing them will cause confusion and more work.

Q: I tried to download a package listed in one of the security advisories, but I got a `file not found' error.

A: Whenever a newer bugfix supersedes an older package on security.debian.org, chances are high that the old package will be removed by the time the new one gets installed. Hence, you'll get this `file not found' error. We don't want to distribute packages with known security bugs longer than absolutely necessary.

Please use the packages from the latest security advisories, which are distributed through the debian-security-announce mailing list. It's best to simply run `apt-get update` before upgrading the package.

Q: I've got a bugfix, can I upload to security.debian.org directly?

A: No, you can't. The archive at security.debian.org is maintained by the security team, who have to approve all packages. You should instead send patches or proper source packages to the security team via team@security.debian.org. They will be reviewed by the security team and eventually uploaded, either with or without modifications.

The Developer's Reference has complete instructions on what to do.

Q: I've got a bugfix, can I upload to proposed-updates instead?

A: Technically speaking, you can. However, you should not do this, since this interferes badly with the work of the security team. Packages from security.debian.org will be copied into the proposed-updates directory automatically. If a package with the same or a higher version number is already installed into the archive, the security update will be rejected by the archive system. That way, the stable distribution will end up without a security update for this package instead, unless the *“wrong”* packages in the proposed-updates directory were rejected. Please contact the security team instead and include all details of the vulnerability and attach the source files (i.e. diff.gz and dsc files) to your mail.

The Developer's Reference has complete instructions on what to do.

Q: I'm pretty sure my packages are fine, how can I upload them?

A: If you are very sure that your packages don't break anything, that the version is sane (i.e. greater than the version in stable and less than the version in testing/unstable), that you didn't change the behaviour of the package, despite the corresponding security problem, that you compiled it for the correct distribution (that is `oldstable-security` or `stable-security`), that the package contains the original source if the package is new on security.debian.org, that you can confirm the patch against the most recent version is clean and only touches the corresponding security problem (check with `interdiff -z` and both `.diff.gz` files), that you have proofread the patch at least thrice, and that `debdiff` doesn't display any changes, you may upload the files into the incoming directory `ftp://ftp.security.upload.debian.org/pub/SecurityUploadQueue` on the security.debian.org directly. Please send a notification with all details and links to team@security.debian.org as well.

Q: How can I help with security?

A: Please review each problem before reporting it to security@debian.org. If you are able to provide patches, that would speed up the process. Do not simply forward bugtraq mails, because we already receive them — but do provide us with additional information about things reported on bugtraq.

A good way to get started with security work is helping out on the Debian Security Tracker (instructions).

Q: What is the scope of proposed-updates?

A: This directory contains packages which are proposed to enter the next revision of Debian stable. Whenever packages are uploaded by a maintainer for the stable distribution, they end up in the proposed-updates directory. Since stable is meant to be stable, no automatic updates are made. The security team will upload fixed packages mentioned in their advisories to stable, however they will be placed in proposed-updates first. Every couple of months the Stable Release Manager checks the list of packages in proposed-updates and discusses whether a package is suited for stable or not. This is compiled into another revision of stable (e.g. 2.2r3 or 2.2r4). Packages that don't fit will probably be rejected and dropped from proposed-updates as well.

Note that the packages uploaded by maintainers (not by the security team) in the proposed-updates/ directory are not supported by the security team.

Q: How is the security team composed?

A: The Debian security team consists of several officers and secretaries. The security team itself appoints people to join the team.

Q: How long will security updates be provided?

A: The security team tries to support a stable distribution for about one year after the next stable distribution has been released, except when another stable distribution is released within this year. It is not possible to support three distributions; supporting two simultaneously is already difficult enough.

Q: How can I check the integrity of packages?

A: This process involve checking the Release file signature against the public key used for the archive. The Release file contains the checksums of Packages and Sources files, which contain checksums of binary and source packages. Detailed instruction on how to check packages integrity can be found in the Debian Securing Manual.

Q: What to do if a random package breaks after a security update?

A: First of all, you should figure out why the package breaks and how it is connected to the security update, then contact the security team if it is serious or the stable release manager if it is less serious. We're talking about random packages that break after a security update of a different package. If you can't figure out what's going wrong but have a correction, talk to the security team as well. You may be redirected to the stable release manager though.

Q: What is a CVE identifier?

A: The Common Vulnerabilities and Exposures project assignes unique names, called CVE identifiers, to specific security vulnerabilities, to make it easier to uniquely refer to a specific issue. More information can be found at Wikipedia.

Q: Does Debian issue a DSA for every CVE id?

A: The Debian security team keeps track of every issued CVE identifier, connect it to the relevant Debian package and assess its impact in a Debian context - the fact that something is assigned a CVE id does not necessarily imply that the issue is a serious threat to a Debian system. This information is tracked in the Debian Security Tracker and for the issues that are considered serious a Debian Security Advisory will be issued.

Low-impact issues not qualifying for a DSA can be fixed in the next release of Debian, in a point release of the current stable or oldstable distributions, or are included in a DSA when that is being issued for a more serious vulnerability.

Q: Can Debian assign CVE identifiers?

A: Debian is a CVE Numbering Authority and can assign ids, but per CVE policy only to yet-undisclosed issues. If you have an undisclosed security vulnerability for software in Debian and would like to get an identifier for it, contact the Debian Security Team. For cases where the vulnerability is already public, we advise to follow the procedure detailed in the CVE OpenSource Request HOWTO.

Q: Does Debian have a vulnerability disclosure policy?

A: Debian has published a vulnerability disclosure policy as part of its participation in the CVE program.

Deprecated Debian security FAQ

Q: What does “local (remote)” mean?

The field *Problem type* in DSA mails is not used since April 2014.
A: Some advisories cover vulnerabilities that cannot be identified with the classic scheme of local and remote exploitability. Some vulnerabilities cannot be exploited from remote, i.e. don't correspond to a daemon listening to a network port. If they can be exploited by special files that could be provided via the network while the vulnerable service is not permanently connected with the network, we write *“local (remote)”* in such cases.

Such vulnerabilities are somewhat between local and remote vulnerabilities and often cover archives that could be provided through the network, e.g. as mail attachment or from a download page.

Home

About
Social Contract
Code of Conduct
Free Software
Partners
Donations
Legal Info
Data Privacy
Contact Us
Help Debian
Site map
Search
The Debian Blog
Debian Micronews
Debian Planet

Getting Debian
Network install
CD/USB ISO images
CD vendors
Pre-installed
Pure Blends
Debian Packages
Developers' Corner

News
Project News
Events
Documentation
Release Info
Installation manual
Debian Books
Debian Wiki

Support
Debian International
Security Information
Bug reports
Mailing Lists
Mailing List Archives
Ports/Architectures

To report a problem with the web site, please e-mail our publicly archived mailing list debian-www@lists.debian.org in English. For other contact information, see the Debian contact page. Web site source code is available.

Last Modified: Mon, May 25 17:56:59 UTC 2020   Last Built: Sun, Dec 19 00:06:12 UTC 2021

Copyright © 1997-2020 SPI and others; See license terms
Debian is a registered trademark of Software in the Public Interest, Inc.