Security bugs

Linux kernel developers take security very seriously. As such, we'd like to know when a security bug is found so that it can be fixed and disclosed as quickly as possible. Please report security bugs to the Linux kernel security team.

Contact

The Linux kernel security team can be contacted by email at <security@kernel.org>. This is a private list of security officers who will help verify the bug report and develop and release a fix. If you already have a fix, please include it with your report, as that can speed up the process considerably. It is possible that the security team will bring in extra help from area maintainers to understand and fix the security vulnerability.

As it is with any bug, the more information provided the easier it will be to diagnose and fix. Please review the procedure outlined in 'Documentation/admin-guide/reporting-issues.rst' if you are unclear about what information is helpful. Any exploit code is very helpful and will not be released without consent from the reporter unless it has already been made public.

Please send plain text emails without attachments where possible. It is much harder to have a context-quoted discussion about a complex issue if all the details are hidden away in attachments. Think of it like a :doc:`regular patch submission <../process/submitting-patches>` (even if you don't have a patch yet): describe the problem and impact, list reproduction steps, and follow it with a proposed fix, all in plain text.

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\admin-guide\(linux-master) (Documentation) (admin-guide)security-bugs.rst`, line 29); *backlink*

Unknown interpreted text role "doc".

Disclosure and embargoed information

The security list is not a disclosure channel. For that, see Coordination below.

Once a robust fix has been developed, the release process starts. Fixes for publicly known bugs are released immediately.

Although our preference is to release fixes for publicly undisclosed bugs as soon as they become available, this may be postponed at the request of the reporter or an affected party for up to 7 calendar days from the start of the release process, with an exceptional extension to 14 calendar days if it is agreed that the criticality of the bug requires more time. The only valid reason for deferring the publication of a fix is to accommodate the logistics of QA and large scale rollouts which require release coordination.

While embargoed information may be shared with trusted individuals in order to develop a fix, such information will not be published alongside the fix or on any other disclosure channel without the permission of the reporter. This includes but is not limited to the original bug report and followup discussions (if any), exploits, CVE information or the identity of the reporter.

In other words our only interest is in getting bugs fixed. All other information submitted to the security list and any followup discussions of the report are treated confidentially even after the embargo has been lifted, in perpetuity.

Coordination

Fixes for sensitive bugs, such as those that might lead to privilege escalations, may need to be coordinated with the private <linux-distros@vs.openwall.org> mailing list so that distribution vendors are well prepared to issue a fixed kernel upon public disclosure of the upstream fix. Distros will need some time to test the proposed patch and will generally request at least a few days of embargo, and vendor update publication prefers to happen Tuesday through Thursday. When appropriate, the security team can assist with this coordination, or the reporter can include linux-distros from the start. In this case, remember to prefix the email Subject line with "[vs]" as described in the linux-distros wiki: <http://oss-security.openwall.org/wiki/mailing-lists/distros#how-to-use-the-lists>

CVE assignment

The security team does not normally assign CVEs, nor do we require them for reports or fixes, as this can needlessly complicate the process and may delay the bug handling. If a reporter wishes to have a CVE identifier assigned ahead of public disclosure, they will need to contact the private linux-distros list, described above. When such a CVE identifier is known before a patch is provided, it is desirable to mention it in the commit message if the reporter agrees.

Non-disclosure agreements

The Linux kernel security team is not a formal body and therefore unable to enter any non-disclosure agreements.