Embargoed hardware issues

Scope

Hardware issues which result in security problems are a different category of security bugs than pure software bugs which only affect the Linux kernel.

Hardware issues like Meltdown, Spectre, L1TF etc. must be treated differently because they usually affect all Operating Systems ("OS") and therefore need coordination across different OS vendors, distributions, hardware vendors and other parties. For some of the issues, software mitigations can depend on microcode or firmware updates, which need further coordination.

Contact

The Linux kernel hardware security team is separate from the regular Linux kernel security team.

The team only handles the coordination of embargoed hardware security issues. Reports of pure software security bugs in the Linux kernel are not handled by this team and the reporter will be guided to contact the regular Linux kernel security team (:ref:`Documentation/admin-guide/ <securitybugs>`) instead.

> **System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\process\[linux-master][Documentation][process]embargoed-hardware-issues.rst`, line 28); *backlink***
>
> Unknown interpreted text role "ref".

The team can be contacted by email at <hardware-security@kernel.org>. This is a private list of security officers who will help you to coordinate an issue according to our documented process.

The list is encrypted and email to the list can be sent by either PGP or S/MIME encrypted and must be signed with the reporter's PGP key or S/MIME certificate. The list's PGP key and S/MIME certificate are available from the following URLs:

- PGP: https://www.kernel.org/static/files/hardware-security.asc
- S/MIME: https://www.kernel.org/static/files/hardware-security.crt

While hardware security issues are often handled by the affected hardware vendor, we welcome contact from researchers or individuals who have identified a potential hardware flaw.

Hardware security officers

The current team of hardware security officers:

- Linus Torvalds (Linux Foundation Fellow)
- Greg Kroah-Hartman (Linux Foundation Fellow)
- Thomas Gleixner (Linux Foundation Fellow)

Operation of mailing-lists

The encrypted mailing-lists which are used in our process are hosted on Linux Foundation's IT infrastructure. By providing this service, members of Linux Foundation's IT operations personnel technically have the ability to access the embargoed information, but are obliged to confidentiality by their employment contract. Linux Foundation IT personnel are also responsible for operating and managing the rest of kernel.org infrastructure.

The Linux Foundation's current director of IT Project infrastructure is Konstantin Ryabitsev.

Non-disclosure agreements

The Linux kernel hardware security team is not a formal body and therefore unable to enter into any non-disclosure agreements. The kernel community is aware of the sensitive nature of such issues and offers a Memorandum of Understanding instead.

Memorandum of Understanding

The Linux kernel community has a deep understanding of the requirement to keep hardware security issues under embargo for coordination between different OS vendors, distributors, hardware vendors and other parties.

The Linux kernel community has successfully handled hardware security issues in the past and has the necessary mechanisms in place to allow community compliant development under embargo restrictions.

The Linux kernel community has a dedicated hardware security team for initial contact, which oversees the process of handling such

issues under embargo rules.

The hardware security team identifies the developers (domain experts) who will form the initial response team for a particular issue. The initial response team can bring in further developers (domain experts) to address the issue in the best technical way.

All involved developers pledge to adhere to the embargo rules and to keep the received information confidential. Violation of the pledge will lead to immediate exclusion from the current issue and removal from all related mailing-lists. In addition, the hardware security team will also exclude the offender from future issues. The impact of this consequence is a highly effective deterrent in our community. In case a violation happens the hardware security team will inform the involved parties immediately. If you or anyone becomes aware of a potential violation, please report it immediately to the Hardware security officers.

Process

Due to the globally distributed nature of Linux kernel development, face-to-face meetings are almost impossible to address hardware security issues. Phone conferences are hard to coordinate due to time zones and other factors and should be only used when absolutely necessary. Encrypted email has been proven to be the most effective and secure communication method for these types of issues.

Start of Disclosure

Disclosure starts by contacting the Linux kernel hardware security team by email. This initial contact should contain a description of the problem and a list of any known affected hardware. If your organization builds or distributes the affected hardware, we encourage you to also consider what other hardware could be affected.

The hardware security team will provide an incident-specific encrypted mailing-list which will be used for initial discussion with the reporter, further disclosure and coordination.

The hardware security team will provide the disclosing party a list of developers (domain experts) who should be informed initially about the issue after confirming with the developers that they will adhere to this Memorandum of Understanding and the documented process. These developers form the initial response team and will be responsible for handling the issue after initial contact. The hardware security team is supporting the response team, but is not necessarily involved in the mitigation development process.

While individual developers might be covered by a non-disclosure agreement via their employer, they cannot enter individual non-disclosure agreements in their role as Linux kernel developers. They will, however, agree to adhere to this documented process and the Memorandum of Understanding.

The disclosing party should provide a list of contacts for all other entities who have already been, or should be, informed about the issue. This serves several purposes:

- The list of disclosed entities allows communication across the industry, e.g. other OS vendors, HW vendors, etc.
- The disclosed entities can be contacted to name experts who should participate in the mitigation development.
- If an expert which is required to handle an issue is employed by an listed entity or member of an listed entity, then the response teams can request the disclosure of that expert from that entity. This ensures that the expert is also part of the entity's response team.

Disclosure

The disclosing party provides detailed information to the initial response team via the specific encrypted mailing-list.

From our experience the technical documentation of these issues is usually a sufficient starting point and further technical clarification is best done via email.

Mitigation development

The initial response team sets up an encrypted mailing-list or repurposes an existing one if appropriate.

Using a mailing-list is close to the normal Linux development process and has been successfully used in developing mitigations for various hardware security issues in the past.

The mailing-list operates in the same way as normal Linux development. Patches are posted, discussed and reviewed and if agreed on applied to a non-public git repository which is only accessible to the participating developers via a secure connection. The repository contains the main development branch against the mainline kernel and backport branches for stable kernel versions as necessary.

The initial response team will identify further experts from the Linux kernel developer community as needed. Bringing in experts can happen at any time of the development process and needs to be handled in a timely manner.

If an expert is employed by or member of an entity on the disclosure list provided by the disclosing party, then participation will be requested from the relevant entity.

If not, then the disclosing party will be informed about the experts participation. The experts are covered by the Memorandum of Understanding and the disclosing party is requested to acknowledge the participation. In case that the disclosing party has a compelling reason to object, then this objection has to be raised within five work days and resolved with the incident team immediately. If the disclosing party does not react within five work days this is taken as silent acknowledgement.

After acknowledgement or resolution of an objection the expert is disclosed by the incident team and brought into the development process.

Coordinated release

The involved parties will negotiate the date and time where the embargo ends. At that point the prepared mitigations are integrated into the relevant kernel trees and published.

While we understand that hardware security issues need coordinated embargo time, the embargo time should be constrained to the minimum time which is required for all involved parties to develop, test and prepare the mitigations. Extending embargo time artificially to meet conference talk dates or other non-technical reasons is creating more work and burden for the involved developers and response teams as the patches need to be kept up to date in order to follow the ongoing upstream kernel development, which might create conflicting changes.

CVE assignment

Neither the hardware security team nor the initial response team assign CVEs, nor are CVEs required for the development process. If CVEs are provided by the disclosing party they can be used for documentation purposes.

Process ambassadors

For assistance with this process we have established ambassadors in various organizations, who can answer questions about or provide guidance on the reporting process and further handling. Ambassadors are not involved in the disclosure of a particular issue, unless requested by a response team or by an involved disclosed party. The current ambassadors list:

ARM	Grant Likely <grant.likely@arm.com>
AMD	Tom Lendacky <tom.lendacky@amd.com>
IBM Z	Christian Borntraeger <borntraeger@de.ibm.com>
IBM Power	Anton Blanchard <anton@linux.ibm.com>
Intel	Tony Luck <tony.luck@intel.com>
Qualcomm	Trilok Soni <tsoni@codeaurora.org>
Microsoft	James Morris <jamorris@linux.microsoft.com>
VMware	
Xen	Andrew Cooper <andrew.cooper3@citrix.com>
Canonical	John Johansen <john.johansen@canonical.com>
Debian	Ben Hutchings <ben@decadent.org.uk>
Oracle	Konrad Rzeszutek Wilk <konrad.wilk@oracle.com>
Red Hat	Josh Poimboeuf <jpoimboe@redhat.com>
SUSE	Jiri Kosina <jkosina@suse.cz>
Amazon	
Google	Kees Cook <keescook@chromium.org>

If you want your organization to be added to the ambassadors list, please contact the hardware security team. The nominated ambassador has to understand and support our process fully and is ideally well connected in the Linux kernel community.

Encrypted mailing-lists

We use encrypted mailing-lists for communication. The operating principle of these lists is that email sent to the list is encrypted either with the list's PGP key or with the list's S/MIME certificate. The mailing-list software decrypts the email and re-encrypts it individually for each subscriber with the subscriber's PGP key or S/MIME certificate. Details about the mailing-list software and the setup which is used to ensure the security of the lists and protection of the data can be found here: https://korg.wiki.kernel.org/userdoc/remail.

List keys

For initial contact see :ref:`Contact`. For incident specific mailing-lists the key and S/MIME certificate are conveyed to the subscribers by email sent from the specific list.

> **System Message: ERROR/3** (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\process\[linux-master][Documentation][process]embargoed-hardware-issues.rst`, **line 288**); ***backlink***
>
> Unknown interpreted text role "ref".

Subscription to incident specific lists

Subscription is handled by the response teams. Disclosed parties who want to participate in the communication send a list of potential subscribers to the response team so the response team can validate subscription requests.

Each subscriber needs to send a subscription request to the response team by email. The email must be signed with the subscriber's PGP key or S/MIME certificate. If a PGP key is used, it must be available from a public key server and is ideally connected to the Linux kernel's PGP web of trust. See also: https://www.kernel.org/signature.html.

The response team verifies that the subscriber request is valid and adds the subscriber to the list. After subscription the subscriber will receive email from the mailing-list which is signed either with the list's PGP key or the list's S/MIME certificate. The subscriber's email client can extract the PGP key or the S/MIME certificate from the signature so the subscriber can send encrypted email to the list.