Management of security issues in CIP

This document explains the methods used by upstream (Debian) and mainline kernel which are a major part of CIP-Core and CIP-Kernel to deal with the CVE cycle.

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2022-11-28	Draft document about Defect management practices in CIP	Sai Ashrith	Dinesh Kumar
002	2022-12-15	Revised document	Sai Ashrith	Dinesh Kumar

Description

CIP CVE scanner is a tool which runs periodically to fetch fixes for CVEs and apply to the repositories. But the security issues are not dealt with directly by CIP but instead depends on upstream to fix the CVEs. The CVE scanner tool used by CIP fetches the fixes reported by the upstream and applies them to the repositories based on the requirement.

Objective

The main objective of this document is to explain the measures taken by Debian and mainline kernel maintainers to meet the defect management requirements (DM-1 to DM-5) as mentioned in IEC-62443-4-1.

Scope

Scope of this document is to consider the defect management practices (DM-1 TO DM-5) used by the upstream maintainers and the methods CIP uses to streamline by fetching and applying those fixes found by upstream in the CIP-Core repository and CIP-Kernel.

CIP does not have a bug tracking system. It relies on upstream projects (Debian and Linux Mainline kernel) for defect management. Following content describes the defect management process in upstream. It is to be noted CIP does not have any control over upstream defect management. ## Defect Management practices

DM-1: Receiving notifications of security-related issues

CIP-Core specific issues are handled and discussed in isar-cip-core. If the applied fixes from the upstream still cause any issue in CIP Kernel, they are recieved in the mailing list.

The Debian Security tracker receives the list of CVEs from MITRE which is a US based not-for-profit company, best known for maintaining CVE id system. It runs a cron job for twice a day and adds the freshly pulled list of CVEs to CVE,DSA and DTSA lists in the data directory.

Debian maintainers receive notifications via debian security tracker mailing list or via the KGB bot in the OFTC network. Many of the CVEs are flagged as NFU(NOT-FOR-US) as the tracker is only concerned about software which are packaged and used on Debian. Nothing is said about a vulnerability affecting a system other than Debian.

The **Linux kernel** developers are ready to take security bugs through mailing list. A bug report is expected because it might help the maintainers to diagnose the issue as quickly as possible. Any exploit code can also sent which will not be released without consent from the reporter unless it is already been made public.

DM-2: Reviewing security-related issues

CIP depends on upstream to handle this process, so below content explains the CVE review system in Debian and mainline linux kernel.

The TODO entries are listed out by **Debian maintainers** after detailed review of all the CVEs added to the data/CVE/list in the tracker repository after MITRE update.

Review happens on all the TODO entries on the condition that the problem issued is affecting Debian. Calculating the severity of the filtered out TODO entry comes later. In this review process, first it is verified that the CVE information is correct based on not just CVE description mentioned by the user but also on research.

If any error is found in the CVE description, it is suggested to write to oss-security mailing list, with a carbon copy (cc) to team@security.debian.org.

Debian's main criteria for assigning a CVE with the NOT-FOR-US flag:

1. If the issue is not related to any software packaged in Debian without Intent or Request for Package tag.
2. Third party modules not yet packaged for Debian even though their parent software is packaged for Debian.
3. Meta packages which only provides a downloader because the code is not present in Debian and no influence on the version.

On the other side if the CVE is not dumped in NFU category, then the review methods are further classified as given below:

1. CVE referring to a Debian package which already has a newer version which already has the fix are noted down with a severity level assigned to it.
2. Undetermined tags are given to the CVEs in case of confidence that it affects one or more packages but there is not enough disclosed references about it. Maintainers can find these undetermined tagged CVEs pooled by the tracker.
3. Issues found in packages that has ITP or RFP tag are made sure to be fixed before the package is put in the debian archive.
4. Duplicates or non-issues are filed with REJECTED tag. In some cases, the vulnerabilities are not fixed with a code change but it is because the package is completely broken. The package is completely removed from the supported Debian releases and tracked in data/packages/removed-packages file to show the failure of consistency checks during new releases.
5. Some CVEs referring to packages which are too old to be supported by the security team are filed with end-of-life tag.

In the final scenario where more work has to be done to find out the affected area, not sure of triaging decision will have their TODO line to explain what investigation has been done on the vulnerability and what needs to done to find the affected area so that other maintainers can review it.

Whereas the **Linux Kernel security team** reviews the bug report, develops and releases a fix. Usually a kernel bug comes with a stack trace which is enough for the developers to find out the line in the source code where the bug occured. So the review stage will not be complex in Linux Kernel when compared to review done on a bug by Debian.

Linux Kernel security team does not assign CVEs as they feel it will drag and delay the bug fixing. If the reporter wants to have a CVE assigned should contact the private linux-distros list.

DM-3: Assessing security-related issues

CIP depends on upstream to handle this process, so below content explains the CVE assessing system followed in upstream.

After deciding the effect of the vulnerability, a severity level is assigned to grade the priority to fix it. Higher priority ones are attended first by the upstream maintainers. Below are different categories representing the severity of a CVE and its criteria :

1. Any source file which is not built for ex: a manual document in doc/foo/examples, if a vulnerability which does not come under security support is given **unimportant** severity level.
2. Problems with less effect for ex: /tmp file races or local DoS are given **low** severity level.
3. User privilege escalation (local & remote) and remote DoS (denial of service) vulnerabilities where code execution happens after user interaction is given **medium** severity level.
4. Anything which allows the attackers to execute haphazard code on a system with or without root privileges is given a **high** severity level. For ex: a vulnerability in a cryptographic package which accepts forged signatures as genuine.

DM-4: Addressing security-related issues

CIP does not explicity solve issues as it acts as a consumer of Debian and mainline Linux kernel. CIP pulls the addressed issues in the upstream and applies them to its components. Below content explains the issue addressing system followed in upstream.

Debian acts as a foundation for other GNU/Linux distributions so vulnerablilities affecting might also affect other distros. So for addressing the issue, Debian coordinates with other parties according to their policy. Just like the members in the distributions list, Debian security team expects expert security researchers to address the vulnerabilites reported.

The **Linux kernel security** developers usually identify the origin of the issue in the source code from the stack trace provided by the reporter. In special cases, security team takes help from area maintainers to fix the vulnerability.

Sensitive bugs which might lead to privilege escalations may need to be coordinated with private mailing list as the distro vendors will be prepared to issue a fixed kernel after disclosure of upstream fix.

DM-5: Disclosing security-related issues

CIP-Core uses Common vulnerability scoring system threat modelling methodologies and uses Debian based wrapper to automatically scan the upstream

repositories using CIP Core CVE Scannerand apply them in CIP.**CIP Kernel** uses CIP Kernel CVE scanner to get the latest CVE fixes and applies to CIP Kernel.

In case of **Debian**, involvment of several parties such as upstream developers and other Linux distributions causes the high variance in time gap between initial report of vulnerability and its public disclosure.Private communication between reporter and Debian security team will cause a lot of friction in progress, Debian security team encourages public disclosure of vulnerabilities even before a fix has been developed.

Linux kernel security team prefers to publish the fix as soon as possible and avoids public discussion about the bug. Slight delay might happen in some cases like the issue is not fully understood, the solution should be tested better and vendor coordination. Developers decide the release date while being in contact with submitter and the vendors. In most cases the time gap between report date and release date will be around 7 days.