CAF Security Advisory Publication Guidelines

May 2013

Table of Contents

CAF Security Advisory Publication

Description

BACKGROUND

Code Aurora Forum (CAF), a Linux Foundation Labs project, is a consortium of companies with projects serving the mobile wireless industry. The projects provide the tested code needed to bring innovative, performance-optimized, open source based projects to market and also serve as a staging area for code that is submitted to the upstream projects.

This document serves as best practice documentation, describing information included in security advisories when published on CAF.

Advisory Overview

The following explains several pieces that make up the final advisory and explains each individual information field as required by the advisory.

ADVISORY HEADER


Multiple issues in DIAG/KGSL system call handling (CVE-2012-4220, CVE-2012-4221, CVE-2012-4222)

Release Date
November 15, 2012

Advisory ID
QCIR-2013-00001-1

Affected Projects
Android for MSM, QRD Android, SIMCOM QRD Android Project

CVE ID(s)
CVE-2012-4220, CVE-2012-4221, CVE-2012-4222

Projects

All Active Projects
Archived Projects

The header of the advisory should be made up by Title, Release Date, Affected Projects, Advisory ID, and CVE ID(s).

Title: A short description of the vulnerability (not the impact), as well as a listing of individual CVE ID(s) as assigned by MITRE or the respective CAF project.

Release Date: Release date of the advisory on CAF. If the advisory is a revision of an old advisory, this should reflect the publication date of the revision.

Affected Projects: A list of CAF projects that are affected by the vulnerability.

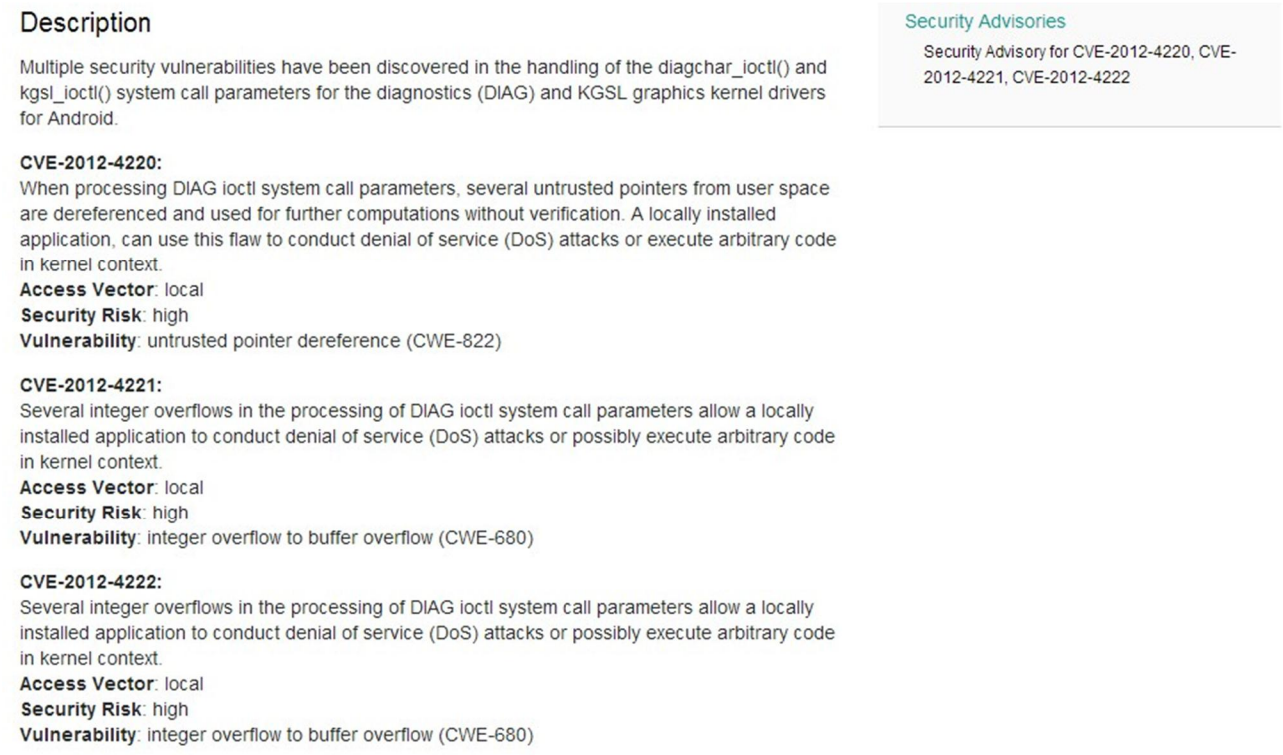
Advisory ID: Each advisory should be identifiable by a unique advisory id. This identifier is assigned by the respective CAF member's security that wishes to publish the advisory. The following scheme shall be used: PREFIX-20XX-YYYYY-REV.

Each entity publishing security advisories on CAF should use its own prefix to identify their advisory. The prefixes are maintained by CAF. Members who did not publish security advisories on CAF should coordinate with the CAF team to prevent double-usage of prefixes.

In the above identifier template, 20XX is the year;YYYYYY is a unique identifier and REV a revision number (starting at 1) that can be used in case there is a need to issue updates for regressions introduced by previous fixes for the vulnerabilities.

CVE ID(s): List of Common Vulnerability and Exposures (CVE) identifiers assigned for the specific vulnerabilities.

ADVISORY BODY



Description

Multiple security vulnerabilities have been discovered in the handling of the diagchar_ioctl() and kgsl_ioctl() system call parameters for the diagnostics (DIAG) and KGSL graphics kernel drivers for Android.

CVE-2012-4220:
When processing DIAG ioctl system call parameters, several untrusted pointers from user space are dereferenced and used for further computations without verification. A locally installed application, can use this flaw to conduct denial of service (DoS) attacks or execute arbitrary code in kernel context.
Access Vector: local
Security Risk: high
Vulnerability: untrusted pointer dereference (CWE-822)

CVE-2012-4221:
Several integer overflows in the processing of DIAG ioctl system call parameters allow a locally installed application to conduct denial of service (DoS) attacks or possibly execute arbitrary code in kernel context.
Access Vector: local
Security Risk: high
Vulnerability: integer overflow to buffer overflow (CWE-680)

CVE-2012-4222:
Several integer overflows in the processing of DIAG ioctl system call parameters allow a locally installed application to conduct denial of service (DoS) attacks or possibly execute arbitrary code in kernel context.
Access Vector: local
Security Risk: high
Vulnerability: integer overflow to buffer overflow (CWE-680)

Security Advisories

Security Advisory for CVE-2012-4220, CVE-2012-4221, CVE-2012-4222

The main part of the advisory should contain details about the vulnerabilities that are addressed with the advisory. Each advisory should come with a high-level **Description** which briefly describes/lists the affected code containing the vulnerability and acknowledges security vulnerability in it.

The section should be followed by a list containing information for each individual vulnerability. Each item in this list has to contain a CVE ID, vulnerability description, access vector, security risk, and vulnerability field.

CVE ID: The list item starts with the CVE ID for this specific vulnerability.

Vulnerability Description: Explain the nature of the vulnerability as well as its impact.

Access Vector: State execution environment as required by the vulnerability to get exploited. This can be either *local* for vulnerabilities that are exploited on-device or *remote* for vulnerabilities that can be triggered via external communication paths such as network protocols.

Security Risk: Quantify the security impact this vulnerability has considering its environment and use cases of the affected code and the vulnerability. Valid values for this field are *low, medium, high,* and *critical*. The meaning of those will be explained later within this document.

Vulnerability: Common Weakness Enumeration (CWE) name followed by its numerical identifier. See: http://cwe.mitre.org/data/index.html.

AFFECTED VERSIONS

In addition to the vulnerability details, the advisory also shall list information of which CAF code bases are affected by the problem.

Affected versions:
The Android releases from CAF prior to November 15, 2012 using Linux kernel from the following heads:

- msm-3.4
- msm-3.0
- jb_*
- ics_*
- gingerbread_*

This can be free-form text listing information about which GIT branches of the projects listed in the advisory header are affected by the problem.

FIX INFORMATION

The previous sections are followed by a section to make general notes concerning the advisory and/or vulnerability as well as listing patches that address the vulnerability.

Note:
Permission changes in ICS and Jelly Bean that restrict /dev/diag access to qcom_diag group mitigate CVE-2012-4220 and CVE-2012-4221.

Patch

We advise customers to apply the following patches:
https://www.codeaurora.org/patches/quic/la/.PATCH_17010_jweEF843feG.tar.gz

Individual Patches

- CVE-2012-4220, CVE-2012-4221 in msm-3.4:
  https://www.codeaurora.org/gitweb/quic/la/?p=kernel/msm.git;a=commit;h=32682d16fb46a60a7952c4d9e0653602ff674e4b
- CVE-2012-4222 in msm-3.4:
  https://www.codeaurora.org/gitweb/quic/la/?p=kernel/msm.git;a=commit;h=1e76f61bb001b93795a227f8f808104b6c10b048

Note: Optional field for general remarks regarding the advisory or the patch information. This can also include mitigations for the vulnerabilities that do not require the patches to be applied.

Patch: The patch sections should link to a tar.gz file hosted on CAF that contains a patch set addressing all vulnerabilities that are listed in the advisory. This should be followed by a section that lists patches on a per-CVE ID basis.

ADVISORY FOOTER

The advisory footer ends the security advisory and gives the opportunity to publicly thank or acknowledge the finder of the security vulnerability and provide other information.

Acknowledgement

Qualcomm Innovation Center, Inc. (QuIC) thanks giantpune@gmail.com for reporting the related issues and working with QuIC to help improve Android device security.

Revisions

Initial security revision

Contact

security-advisory@quicinc.com

Acknowledgement: Free form text field to include acknowledgement notes and list the finder(s) of the respective issues.

Revisions: Free form text field stating whether this is a revision of a previously issued advisory and if so, it should list the advisory id of previous revisions. In this case, the original advisory id has to be used and the revision id has to be incremented by one.

Contact: Security contact of the respective CAF member that can be used by researchers and other organizations to acquire more information about the published advisory, make comments, or report further issues.

Security Risk Rating

Each vulnerability included in the advisory comes with an associated security risk rating. Ratings that should be used are *low, medium, high*, and *critical*. Following are brief descriptions of these severity levels.

RISK RATING LEVELS

Critical

Critical vulnerabilities may allow an attacker to gain full control of a device remotely; typically by sending malicious payload that is received and processed by the device. Examples for this are vulnerabilities in kernel/driver code or applications running in a privileged context that provides means for remote communication to other services, applications, or users.

A vulnerability that enables an attacker permanently or over an extended period of time to disable device functionality remotely and cause device unusable also falls into this category. In this case, an impacted device normally cannot be recovered from a hardware reset.

Vulnerabilities that allow bypassing or disabling a critical security mechanism either locally or remotely are also covered by this category. Examples for this include compromises of secure

execution environment, secure boot bypasses, and universal methods that allow bypassing exploit mitigation mechanisms such as ASLR or DEP.

High

High vulnerabilities may allow an attacker to achieve privilege escalation such as rooting through local access; to execute arbitrary code and allow to access confidential information such as device secrets or user credentials through execution of code via local access. Examples for confidential device information may include contents of hardware keys, location information that is of user privacy concern, or contents of secure storage.

This category also includes remotely triggered temporary denial of service vulnerabilities that lead to a device crash (reboot) or hang.

Medium

Medium vulnerabilities may allow an attacker to achieve similar impact to the ones in the High category, but require additional user interaction or another vulnerability to work together. Examples of this category include device rooting that requires an elevated privilege above normal user privilege.

Additionally this category comprises of vulnerabilities that allow an attacker to access sensitive, but not security critical information such as firmware versions, IMEI, IMSI, or phone numbers for mobile devices.

Low

Low vulnerabilities are security vulnerabilities that do not directly cause harm to the user or the device. This includes access to general information such as general device settings or device specific details.

Vulnerabilities that itself do not qualify for any of the above categories, but may add to the overall impact of another vulnerability and elevate its effect also fall into this category.

This category also includes Defense-in-Depth issues that do not have an attack vector at the time of issue discovery; but improved code can mitigate the attack if other defense measures fall.

The rating of individual cases may differ from the above guideline if other information becomes available such as the existence of an exploit in the wild exploiting the vulnerability. The exact risk rating to be used for the advisory should be determined in coordination with the security team of the respective CAF member.