|  |  |
| --- | --- |
| Product name | Confidentiality level |
| VOG-L29 | CONFIDENTIAL |
| Commercial Name | Total 9 pages |
| HUAWEI P30 Pro |

HUAWEI VOG-L29 9.1.0.193(C432E4R2P2) Software Release Notes

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by | *VOG Team* | Date | 2019-08-05 |
| Reviewed by | *VOG Team* | Date | 2019-08-05 |
| Approved by | *VOG Team* | Date | 2019-08-05 |



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Revision version | Change Description | Author |
| *yyyy-mm-dd* | *1.0* | *Release for version V100R001CXXB001* | *XXX TEAM* |
| *yyyy-mm-dd* | *1.1* | *Add OTA feature description* | *XXX TEAM* |
| *yyyy-mm-dd* | *2.0* | *Release for version V100R001CXXB002* | *XXX TEAM* |
| *2018-2-13* | *2.1* | *1. Change “Product version” to “Commercial Name”*  *2. Remove “Main features”*  *3. Make “Version Description” more clear*  *4.Change” Improvement in the Previous Version” to “Improvement From the Previous Version”*  *4.Change “Effect” to “Remarks”* | *MR TEAM* |
| *2018-5-18* | *2.2* | *Add match EMUI 9.0 template* | *Custom Team* |
| *2018-8-8* | *2.2* | *1. Delete column “Case ID”*  *2. Change “Issue Description” to “Feature Description” in New Features* | *MR TEAM* |
| *2019-1-1* | *2.3* | *1. Add “IMEI SV” in Version Description.* | *MR TEAM* |
| *2019-3-12* | *2.3.1* | *1. Update Version Description.* | *I&M* |
| *2019-5-17* | *2.3.2* | *1. Add “Android security patch”* | *I&M* |

Table of Contents

[1 Version Description 4](#_Toc509496825)

[2 New Features 4](#_Toc509496826)

[3 Improvement from the Previous Version 4](#_Toc509496827)

[4 Known Limitations and Issues 5](#_Toc509496828)

[5 Software Vulnerabilities Fixes 5](#_Toc509496829)

***VOG-L29 9.1.0.193(C432E4R2P2) Software Release Notes***

# Version Description

|  |  |
| --- | --- |
| Model | *VOG-L29* |
| Current version | *9.1.0.193(C432E4R2P2)* |
| Previous version | *9.1.0.185(C432E4R2P2)* |
| IMEI SV | 13 |
| OS version | 9 |
| EMUI version | 9.1.0 |
| CPU | *Huawei Kirin 980* |
| Android Security Patch | *1 August 2019* |
| Baseband version | *21C20B370S000C000, 21C20B370S000C000* |
| Kernel Version | *4.9.148*  *android@localhost #1*  *Mon Aug 5 12:26:07 CST 2019* |
| Version Type | *MR6* |

# New Features

| **Index** | **Feature Description** |
| --- | --- |
| 1 | Adds Night mode to the front camera, for clearer and more vibrant night photography. |
| 2 | Adds the Gallery video editing function, allowing for creative and fine-tuned videos. |
| 3 | Adds support for HUAWEI X Gentle Monster intelligent eyewear, providing a uniquely fashionable, technologically-advanced, and interactive new experience. |
| 4 | Integrates Android security patches released in August 2019 for improved system security. |

# Improvement from the Previous Version

| **Index** | **Issue Description** |
| --- | --- |
| 1 | Elisa SIM VoLTE, enable CF, 4G signal dropped |
| 2 | Elisa SIM VoWiFi with airplane mode, cannot enable CF. |

# Known Limitations and Issues

| Index | Issue Description | Remarks |
| --- | --- | --- |
| 1 | Vodafone Fails to Consolidate Multi-Party Calls in Volte | Agree fix on next version |

# Software Vulnerabilities Fixes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Software/Module name | Version | CVE ID | Vulnerability Description | Impact Description |
| Platform | 9 | CVE-2019-2121 | In ActivityManagerService.attachApplication of ActivityManagerService, there is a possible race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to detect and handle the synchronization issues correctly. |
| Qualcomm components | NA | CVE-2019-10499 |  |  |
| Qualcomm closed-source components | NA | CVE-2019-10539 |  |  |
| Qualcomm closed-source components | NA | CVE-2019-10540 |  |  |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2017-13177 | In multiple hand-crafted functions in libhevc, NEON registers are not preserved, leading to possible remote code execution. | The fix is designed to preserve the NEON registers, as required by the ARM ABI calling conventions. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2017-13279 | In M3UParser::parse of libstagefright, there is a memory resource exhaustion due to a large loop of pushing items into a vector. This could lead to a remote denial of service of a critical component. | The fix is designed to detect the out of memory condition and fail cleanly. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2018-9350 | In ih264d\_delete\_st\_node\_or\_make\_lt of ih264d\_dpb\_mgr.c there is a possible out of bounds read due to uninitialized data. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to avoid out of bounds read. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2136 | In Status::readFromParcel of Status.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to add proper bounds check. |
| Platform | 9 | CVE-2019-2137 | In the endCall() function of TelecomManager.java, there is a possible Denial of Service due to a missing permission check. This could lead to local denial of access to Emergency Services with User execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to add the appropriate check. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2128 | In ACELP\_4t64\_fx of c4t64fx.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to add the missing bounds check. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2130 | In CompilationJob::FinalizeJob of compiler.cc, there is a possible remote code execution due to type confusion. This could lead to escalation of privilege from a malicious proxy configuration with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to disable the optimizing compiler for PAC files. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2133 | In Mfc\_Transceive of phNxpExtns\_MifareStd.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to add a bounds check to avoid integer overflow. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2134 | In phFriNfc\_ExtnsTransceive of phNxpExtns\_MifareStd.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to add a bounds check to avoid overflow. |
| Qualcomm closed-source components | NA | CVE-2019-10489 |  |  |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2129 | In extract3GPPGlobalDescriptions of TextDescriptions.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to add the missing bounds check. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2127 | In AudioInputDescriptor::setClientActive of AudioInputDescriptor.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to change references to AudioMix to use refcounted AudioPolicyMix. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2135 | In Mfc\_Transceive of phNxpExtns\_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to add proper bounds check. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2122 | In LockTaskController.lockKeyguardIfNeeded of the LockTaskController.java, there was a difference in the handling of the default case between the WindowManager and the Settings. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to have both the LockTaskController and ScreenPinningSettings components use the same default logic. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2126 | In ParseContentEncodingEntry of mkvparser.cc, there is a possible double free due to a missing reset of a freed pointer. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to correctly initialize and clear the pointer. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2132 | It is possible to overlay the VPN dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to protect VPN dialogs against overlays. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2120 | In OatFileAssistant::GenerateOatFile of oat\_file\_assistant.cc, there is a possible file corruption issue due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to correctly set the initial permissions on the directory. |
| Broadcom components | NA | CVE-2019-11516 | In some Broadcom Bluetooth chips, there is possible memory corruption due to a heap buffer overflow. This could lead to remote code execution over Bluetooth while the user is scanning for devices, with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to update the Broadcom Bluetooth firmware. |
| Qualcomm closed-source components | NA | CVE-2019-2294 |  |  |
| Qualcomm components | NA | CVE-2019-10492 |  |  |
| Qualcomm components | NA | CVE-2019-10509 |  |  |
| Qualcomm components | NA | CVE-2019-10510 |  |  |
| Qualcomm components | NA | CVE-2019-10538 |  |  |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2125 | In ChangeDefaultDialerDialog.java, there is a possible escalation of privilege due to an overlay attack. This could lead to local escalation of privilege, granting privileges to a local app without the user's informed consent, with no additional privileges needed. User interaction is needed for exploitation. | The fix is designed to protect the confirmation dialog from being overlayed. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-2131 | An application with overlay permission can display overlays on top of settings UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | The fix is designed to not allow applications to draw overlays on top of settings UI. |
| Platform | 7.0,7.1.1,7.1.2,8.0,8.1,9 | CVE-2019-9506 | In some bluetooth controllers, there is a possible way for an attacker to create an insecure connection due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | The fix is designed to disallow the potentially insecure usage of crypto. |