|  |  |
| --- | --- |
| Product name | Confidentiality level |
| MT7-TL10 |  |
| Product version | Total 5 pages |
| MT7-TL10C636B512 |

MT7-TL10 Software Release Notes V1.0

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by | *MT7-EMUI4.0 Team* | Date | *2015-12-25* |
| Reviewed by | *MT7-EMUI4.0 Team* | Date | *2015-12-25* |
| Approved by | *MT7-EMUI4.0 Team* | Date | *2015-12-25* |



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Revision version | Software version | Change Description | Author |
| *2015-12-25* | *1.0* | *C636B512* | *Release for version C636B512* | *MT7-EMUI4.0 TEAM* |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 Main Features 4](#_Toc438047805)

[2 Software 4](#_Toc438047806)

[**2.1** **Version Description** 4](#_Toc438047807)

[**2.2** **New Features** 4](#_Toc438047808)

[**2.3** **Improvement in the Previous Version** 4](#_Toc438047809)

[**2.4** **Known Limitations and Issues** 5](#_Toc438047810)

[3 Software Vulnerabilities Fixes 5](#_Toc438047811)

***MT7-TL10 Software Release Notes V1.0***

|  |  |
| --- | --- |
| Abbreviations | Description |
|  |  |
|  |  |

# Main Features

The *MT7-TL10C636B512* supports the following standards:

| Item | Specifications |
| --- | --- |
| *NFC* |  |
| *BT* |  |
| *Whether Forecast* |  |
| *Dual Sim* |  |
| *CVAA* |  |

# Software

## **Version Description**

|  |  |
| --- | --- |
| Current Version | *MT7-TL10C636B512* |
| Previous Version |  |
| OS | Google Android |
| OS Version | *6.0* |
| Baseline Information |  |

## **New Features**

| **Index** | **Case ID** | **Issue Description** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |

## **Improvement in the Previous Version**

| **Index** | **Case ID** | **Issue Description** |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |

## **Known Limitations and Issues**

| Index | Issue Description | Effect |
| --- | --- | --- |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

# Software Vulnerabilities Fixes

*[Software Vulnerabilities include Android Vulnerability, Third-party software Vulnerability, and Huawei Vulnerability]*

*[Android Vulnerability is from Google, which reported publicly.]*

*[Third-party software is a type of computer software that is sold together with or provided for free in Huawei products or solutions with the ownership of intellectual property rights (IPR) held by the original contributors. Third-party software can be but is not limited to: Purchased software, Software that is built in or attached to purchased hardware, Software in products of the original equipment manufacturer (OEM) or original design manufacturer (ODM), Software that is developed with technical contribution from partners (ownership of IPR all or partially held by the partners), Software that is legally obtained free of charge.*

*The data of third-party software vulnerabilities fixes can be exported from PDM.*

*If the table is excessively long, you can divide it into multiple ones by product version, or deliver it in an excel file with patch release notes and provide reference information in this section.]*

*[Huawei Vulnerability is Huawei own software’ Vulnerability, which found by outside]*

*Vulnerabilities information is available through CVE IDs in NVD (National Vulnerability Database) website:* [*http://web.nvd.nist.gov/view/vuln/search*](http://web.nvd.nist.gov/view/vuln/search)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Software/Module name | Version | CVE ID | Vulnerability Description | Impact Description |
| Android | Android5.1 and below | CVE-2015-1538 | Integer overflows during MP4 atom processing. | Could potentially lead to remote code execution. |
| Android | Android5.1 and below | CVE-2015-1539 | An integer underflow in ESDS. | Could potentially lead to remote code execution. |
| Android | Android 4.4 and above | CVE-2015-3824 | Integer overflow in libstagefright when parsing the MPEG4 tx3g atom. | This may be exploited to gain media\_server privileges. |
| Android | Android 4.4 and above | CVE-2015-3827 | Integer underflow in libstagefright when processing MPEG4 covr atoms | This may be exploited to gain media\_server privileges |
| Android | Android 5.0 and above | CVE-2015-3828 | Integer underflow in libstagefright if size is below 6 while processing 3GPP metadata. | This may be exploited to gain media\_server privileges. |
| Android | Android 4.4 and above | CVE-2015-3829 | Integer overflow in libstagefright processing MPEG4 covr atoms when chunk\_data\_size is SIZE\_MAX. | This may be exploited to gain media\_server privileges. |
| Android | Android 5.0 and above | CVE-2015-3826 | Unbounded buffer read in libstagefright while parsing 3GPP metadata allows reading arbitrary memory. | This may be exploited to defeat ASLR in processes with media\_server privileges. |