



CVE-2018-7907

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|----------------------------------------------------------------------------------------------------|
| CVE | CVE-2018-7907 |
| State | PUBLIC |
| Assigner | psirt@huawei.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-09-26 13:29:00 UTC |
| Updated | 2018-11-28 16:52:00 UTC |
| Description | Some Huawei products Agassi-L09 AGS-L09C100B257CUSTC100D001, AGS-L09C170B253CUSTC170D001, AGS-L09C |

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------------------|-----------------------------|--------|---------|----------|
| Hardware | Huawei | Agassi-I09 | - | All | All | All |
| Hardware | Huawei | Agassi-I09 | - | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c100b257custc100d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c170b253custc170d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c199b251custc199d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c229b003custc229d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c100b257custc100d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c170b253custc170d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c199b251custc199d001 | All | All | All |
| Operating System | Huawei | Agassi-I09 Firmware | ags-I09c229b003custc229d001 | All | All | All |
| Hardware | Huawei | Agassi-w09 | - | All | All | All |
| Hardware | Huawei | Agassi-w09 | - | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c100b257custc100d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c128b252custc128d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c170b252custc170d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c229b251custc229d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c331b003custc331d001 | All | All | All |

| | | | | | | |
|------------------|--------|---------------------------------------|-----------------------------|-----|-----|-----|
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c794b001custc794d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c100b257custc100d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c128b252custc128d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c170b252custc170d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c229b251custc229d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c331b003custc331d001 | All | All | All |
| Operating System | Huawei | Agassi-w09 Firmware | ags-w09c794b001custc794d001 | All | All | All |
| Hardware | Huawei | Baggio2-u01a | - | All | All | All |
| Hardware | Huawei | Baggio2-u01a | - | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c100b160custc100d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c170b160custc170d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c199b162custc199d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c209b160custc209d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c333b160custc333d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c100b160custc100d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c170b160custc170d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c199b162custc199d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c209b160custc209d001 | All | All | All |
| Operating System | Huawei | Baggio2-u01a Firmware | bg2-u01c333b160custc333d001 | All | All | All |
| Hardware | Huawei | Bond-al00c | - | All | All | All |
| Hardware | Huawei | Bond-al00c | - | All | All | All |
| Operating System | Huawei | Bond-al00c Firmware | bond-al00cc00b201 | All | All | All |
| Operating System | Huawei | Bond-al00c Firmware | bond-al00cc00b201 | All | All | All |
| Hardware | Huawei | Bond-al10b | - | All | All | All |
| Hardware | Huawei | Bond-al10b | - | All | All | All |
| Operating System | Huawei | Bond-al10b Firmware | bond-al10bc00b201 | All | All | All |
| Operating System | Huawei | Bond-al10b Firmware | bond-al10bc00b201 | All | All | All |
| Hardware | Huawei | Bond-tl10b | - | All | All | All |
| Hardware | Huawei | Bond-tl10b | - | All | All | All |
| Operating System | Huawei | Bond-tl10b Firmware | bond-tl10bc01b201 | All | All | All |
| Operating System | Huawei | Bond-tl10b Firmware | bond-tl10bc01b201 | All | All | All |
| Hardware | Huawei | Bond-tl10c | - | All | All | All |
| Hardware | Huawei | Bond-tl10c | - | All | All | All |
| Operating System | Huawei | Bond-tl10c Firmware | bond-tl10cc01b131 | All | All | All |
| Operating System | Huawei | Bond-tl10c Firmware | bond-tl10cc01b131 | All | All | All |

| | | | | | | |
|------------------|--------|-----------------------|-----------------------------|-----|-----|-----|
| Hardware | Huawei | Haydn-I1jb | - | All | All | All |
| Hardware | Huawei | Haydn-I1jb | - | All | All | All |
| Operating System | Huawei | Haydn-I1jb Firmware | hdn-I1jc137b068 | All | All | All |
| Operating System | Huawei | Haydn-I1jb Firmware | hdn-I1jc137b068 | All | All | All |
| Hardware | Huawei | Kobe-I09a | - | All | All | All |
| Hardware | Huawei | Kobe-I09a | - | All | All | All |
| Hardware | Huawei | Kobe-I09ahn | - | All | All | All |
| Hardware | Huawei | Kobe-I09ahn | - | All | All | All |
| Operating System | Huawei | Kobe-I09ahn Firmware | kob-I09c233b226 | All | All | All |
| Operating System | Huawei | Kobe-I09ahn Firmware | kob-I09c233b226 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c100b252custc100d001 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c209b002custc209d001 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c362b001custc362d001 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c100b252custc100d001 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c209b002custc209d001 | All | All | All |
| Operating System | Huawei | Kobe-I09a Firmware | kob-I09c362b001custc362d001 | All | All | All |
| Hardware | Huawei | Kobe-w09c | - | All | All | All |
| Hardware | Huawei | Kobe-w09c | - | All | All | All |
| Operating System | Huawei | Kobe-w09c Firmware | kob-w09c128b251custc128d001 | All | All | All |
| Operating System | Huawei | Kobe-w09c Firmware | kob-w09c128b251custc128d001 | All | All | All |
| Hardware | Huawei | Lelandp-I22c | - | All | All | All |
| Hardware | Huawei | Lelandp-I22c | - | All | All | All |
| Operating System | Huawei | Lelandp-I22c Firmware | 8.0.0.101_c675custc675d2 | All | All | All |
| Operating System | Huawei | Lelandp-I22c Firmware | 8.0.0.101_c675custc675d2 | All | All | All |
| Hardware | Huawei | Lelandp-I22d | - | All | All | All |
| Hardware | Huawei | Lelandp-I22d | - | All | All | All |
| Operating System | Huawei | Lelandp-I22d Firmware | 8.0.0.101_c675custc675d2 | All | All | All |
| Operating System | Huawei | Lelandp-I22d Firmware | 8.0.0.101_c675custc675d2 | All | All | All |
| Hardware | Huawei | Rhone-al00 | - | All | All | All |
| Hardware | Huawei | Rhone-al00 | - | All | All | All |
| Operating System | Huawei | Rhone-al00 Firmware | rhone-al00c00b186 | All | All | All |
| Operating System | Huawei | Rhone-al00 Firmware | rhone-al00c00b186 | All | All | All |
| Hardware | Huawei | Selina-I02 | - | All | All | All |
| Hardware | Huawei | Selina-I02 | - | All | All | All |
| Operating System | Huawei | Selina-I02 Firmware | selina-I02c432b153 | All | All | All |

| | | | | | | |
|------------------|--------|------------------------|-----------------------|-----|-----|-----|
| Operating System | Huawei | Selina-I02 Firmware | selina-i02c432b153 | All | All | All |
| Hardware | Huawei | Stanford-I09s | - | All | All | All |
| Hardware | Huawei | Stanford-I09s | - | All | All | All |
| Operating System | Huawei | Stanford-I09s Firmware | stanford-i09sc432b183 | All | All | All |
| Operating System | Huawei | Stanford-I09s Firmware | stanford-i09sc432b183 | All | All | All |
| Hardware | Huawei | Toronto-al00 | - | All | All | All |
| Hardware | Huawei | Toronto-al00 | - | All | All | All |
| Hardware | Huawei | Toronto-al00a | - | All | All | All |
| Hardware | Huawei | Toronto-al00a | - | All | All | All |
| Operating System | Huawei | Toronto-al00a Firmware | toronto-al00ac00b223 | All | All | All |
| Operating System | Huawei | Toronto-al00a Firmware | toronto-al00ac00b223 | All | All | All |
| Operating System | Huawei | Toronto-al00 Firmware | toronto-al00c00b223 | All | All | All |
| Operating System | Huawei | Toronto-al00 Firmware | toronto-al00c00b223 | All | All | All |
| Hardware | Huawei | Toronto-tl10 | - | All | All | All |
| Hardware | Huawei | Toronto-tl10 | - | All | All | All |
| Operating System | Huawei | Toronto-tl10 Firmware | toronto-tl10c01b223 | All | All | All |
| Operating System | Huawei | Toronto-tl10 Firmware | toronto-tl10c01b223 | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------------------------------------------------------------------|---------|----------------------------------------------------|---------------------|
| Security Advisory - Sensitive Information Leak Vulnerability in Some Huawei Products | CONFIRM | www.huawei.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

CVE.report and Source URL Uptime Status status.cve.report