CVE-2014-8571

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-8571
State	PUBLISHED
Assigner	huawei
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-02 20:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Apps on Huawei Ascend P6 mobile phones with software EDGE-U00 V100R001C17B508SP01 and earlier versions before

Risk And Classification

Primary CVSS: v3.0 3.3 LOW from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Problem Types: CWE-264 | Screen Capture

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	3.3	LOW	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	Ascend P6 Edge-c00	-	All	All	All
Operating System	Huawei	Ascend P6 Edge-c00 Firmware	All	All	All	All
Hardware	Huawei	Ascend P6 Edge-t00	-	All	All	All
Operating System	Huawei	Ascend P6 Edge-t00 Firmware	All	All	All	All
Hardware	Huawei	Ascend P6 Edge-u00	-	All	All	All
Operating System	Huawei	Ascend P6 Edge-u00 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product
CNA	Na	EDGE-U00EDGE-T00EDGE-C00 EDGE-U00 V100R001C17B508SP01 And Earlier VersionsV100R001C17B508SP02ED

References

Reference	Source	Link
Security Advisory-Screen Capture Vulnerability on Huawei Ascend P6 Mobile Phones	af854a3a-2127-422b-91ae-364da2661108	www.hu
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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