



CVE-2015-7888

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

Summary

CVE	CVE-2015-7888
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-07 14:29:00 UTC
Updated	2017-06-14 14:49:00 UTC
Description	Directory traversal vulnerability in the WifiHs20UtilityService on the Samsung S6 Edge LRX22G.G925VVRU1AOE2 allows

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Samsung	Galaxy S6 Edge	-	All	All	All
Hardware	Samsung	Galaxy S6 Edge	-	All	All	All
Operating System	Samsung	Galaxy S6 Edge Firmware	g925vvr1aoe2	All	All	All
Operating System	Samsung	Galaxy S6 Edge Firmware	g925vvr1aoe2	All	All	All

References

Reference	Source	Link	Tags
Samsung WifiHs20UtilityService Path Traversal ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Adv
Samsung Galaxy S6 CVE-2015-7888 Directory Traversal Vulnerability	BID	www.securityfocus.com	Third Party Adv
Issue 489 - project-zero - Samsung WifiHs20UtilityService path traversal - Monorail	MISC	bugs.chromium.org	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)