

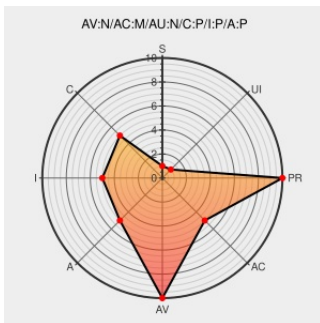


CVE-2015-5991

Published on: 09/21/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5991

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kasda Kw58293](#) from [Philippine Long Distance Telephone](#) contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in form2WlanSetup.cgi on Philippine Long Distance Telephone (PLDT) SpeedSurf 504AN devices with firmware GAN9.8U26-4-TX-R6B018-PH.EN and Kasda KW58293 devices allows remote attackers to hijack the authentication of administrators for requests that perform setup operations, as demonstrated by modifying network settings.

CVE-2015-5991 has been assigned by cert@cert.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Vulnerability Note VU#525276 - Philippine Long Distance Telephone SpeedSurf 504AN and Kasda KW58293 contain multiple vulnerabilities	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#525276

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Philippine Long Distance Telephone	Kasda Kw58293	All	All	All	All
Hardware 	Philippine Long Distance Telephone	Kasda Kw58293	All	All	All	All
Hardware 	Philippine Long Distance Telephone	Kasda Kw58293 Firmware	-	All	All	All
Hardware 	Philippine Long Distance Telephone	Kasda Kw58293 Firmware	-	All	All	All
Hardware 	Philippine Long Distance Telephone	Speedsurf 504an	All	All	All	All
Hardware 	Philippine Long Distance Telephone	Speedsurf 504an	All	All	All	All
Operating System	Philippine Long Distance Telephone	Speedsurf 504an Firmware	gan9.8u26-4-tx-r6b018-hp.en	All	All	All
Operating System	Philippine Long Distance Telephone	Speedsurf 504an Firmware	gan9.8u26-4-tx-r6b018-hp.en	All	All	All
cpe:2.3:h:philippine_long_distance_telephone:kasda_kw58293:~::~::~::~:						
cpe:2.3:h:philippine_long_distance_telephone:kasda_kw58293:~::~::~::~:						
cpe:2.3:h:philippine_long_distance_telephone:kasda_kw58293_firmware:-:~::~::~::~:						
cpe:2.3:h:philippine_long_distance_telephone:kasda_kw58293_firmware:-:~::~::~::~:						
cpe:2.3:h:philippine_long_distance_telephone:speedsurf_504an:~::~::~::~:						
cpe:2.3:h:philippine_long_distance_telephone:speedsurf_504an:~::~::~::~:						
cpe:2.3:o:philippine_long_distance_telephone:speedsurf_504an_firmware:gan9.8u26-4-tx-r6b018-hp.en:~::~::~::~:						
cpe:2.3:o:philippine_long_distance_telephone:speedsurf_504an_firmware:gan9.8u26-4-tx-r6b018-hp.en:~::~::~::~:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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