



CVE-2018-13032

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

Summary

CVE	CVE-2018-13032
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-01 16:29:00 UTC
Updated	2018-08-31 20:07:00 UTC
Description	ECESSA ShieldLink SL175EHQ 10.7.4 devices have CSRF to add superuser accounts via the cgi-bin/pl_web.cgi/util_config

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ecessa	Shieldlink SL175ehq	-	All	All	All
Hardware	Ecessa	Shieldlink SL175ehq	-	All	All	All
Operating System	Ecessa	Shieldlink SL175ehq Firmware	10.7.4	All	All	All
Operating System	Ecessa	Shieldlink SL175ehq Firmware	10.7.4	All	All	All

References

Reference	Source	Link
Ecessa ShieldLink SL175EHQ < 10.7.4 - Cross-Site Request Forgery (Add Superuser) - Hardware webapps Exploit	EXPLOIT-DB	www.exploit-db.com/exploits/42842/
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/CVE-2018-13032
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2018-13032

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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