



CVE-2017-7689

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

Summary

CVE	CVE-2017-7689
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-11 21:59:00 UTC
Updated	2022-02-02 02:13:00 UTC
Description	A Command Injection vulnerability in Schneider Electric homeLYnk Controller exists in all versions before 1.5.0.

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Schneider-electric	Homelynk Controller Lss100100	-	All	All	All
Operating System	Schneider-electric	Homelynk Controller Lss100100 Firmware	All	All	All	All
Hardware	Schneider Electric	Homelynk Controller Lss100100	-	All	All	All
Hardware	Schneider Electric	Homelynk Controller Lss100100	-	All	All	All
Operating System	Schneider Electric	Homelynk Controller Lss100100 Firmware	All	All	All	All

References

Reference	Source	Link
download.schneider-electric.com/files	CONFIRM	download.schneider-electric.com
Schneider Electric homeLYnk Controller (Update A) ICS-CERT	MISC	ics-cert.us-cert.gov
Schneider Electric homeLYnk Controller CVE-2017-7689 Command Injection Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)