



# CVE-2017-5157

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-5157
<b>State</b>	PUBLIC
<b>Assigner</b>	ics-cert@hq.dhs.gov
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-13 21:59:00 UTC
<b>Updated</b>	2022-01-31 20:16:00 UTC
<b>Description</b>	An issue was discovered in Schneider Electric homeLYnk Controller, LSS100100, all versions prior to V1.5.0. The homeLYnk Controller LSS100100 is a hardware device that is used to control and monitor industrial processes. The issue is a cross-site scripting (XSS) vulnerability that allows an attacker to inject malicious code into the web interface of the device. This code can be used to steal sensitive information, such as passwords and session cookies, and to perform other malicious actions. The issue is caused by a lack of proper input validation and output encoding in the web interface. The issue is tracked in the ICS-CERT advisory ICSA-17-019-01A.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Schneider-electric	Homelynk Controller Lss100100	-	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	1.3.0	All	All	All
Operating System	Schneider Electric	Homelynk Controller Lss100100 Firmware	1.3.0	All	All	All

## References

Reference	Source	Link	Tag
ICS-CERT Advisories   ICS-CERT	MISC	<a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>	Thir
Schneider homeLYnk Controller LSS1001003 CVE-2017-5157 Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Thir
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[590518](#) Schneider Electric homeLYnk Controller (Update A) Multiple Vulnerabilities (ICSA-17-019-01A)

© [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](#)**