



# CVE-2018-16946

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

## Summary

<b>CVE</b>	CVE-2018-16946
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-09-12 01:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	LG LNB*, LND*, LNU*, and LNV* smart network camera devices have broken access control. Attackers are able to downlo

## Risk And Classification

**Problem Types:** CWE-552

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Lg	Lnb5110	-	All	All	All
Hardware	Lg	Lnb5110	-	All	All	All
Operating System	Lg	Lnb5110 Firmware	All	All	All	All
Hardware	Lg	Lnb5320	-	All	All	All
Hardware	Lg	Lnb5320	-	All	All	All
Hardware	Lg	Lnb5320r	-	All	All	All
Hardware	Lg	Lnb5320r	-	All	All	All
Operating System	Lg	Lnb5320r Firmware	All	All	All	All
Operating System	Lg	Lnb5320 Firmware	All	All	All	All
Hardware	Lg	Lnb7210	-	All	All	All
Hardware	Lg	Lnb7210	-	All	All	All
Operating System	Lg	Lnb7210 Firmware	All	All	All	All
Hardware	Lg	Lnd3230r	-	All	All	All
Hardware	Lg	Lnd3230r	-	All	All	All
Operating System	Lg	Lnd3230r Firmware	All	All	All	All
Hardware	Lg	Lnd5110	-	All	All	All
Hardware	Lg	Lnd5110	-	All	All	All

	-					
Hardware	Lg	Lnd5110r	-	All	All	All
Hardware	Lg	Lnd5110r	-	All	All	All
Operating System	Lg	Lnd5110r Firmware	All	All	All	All
Operating System	Lg	Lnd5110 Firmware	All	All	All	All
Hardware	Lg	Lnd5220r	-	All	All	All
Hardware	Lg	Lnd5220r	-	All	All	All
Operating System	Lg	Lnd5220r Firmware	All	All	All	All
Hardware	Lg	Lnd7210	-	All	All	All
Hardware	Lg	Lnd7210	-	All	All	All
Hardware	Lg	Lnd7210r	-	All	All	All
Hardware	Lg	Lnd7210r	-	All	All	All
Operating System	Lg	Lnd7210r Firmware	All	All	All	All
Operating System	Lg	Lnd7210 Firmware	All	All	All	All
Hardware	Lg	Lnu3230r	-	All	All	All
Hardware	Lg	Lnu3230r	-	All	All	All
Operating System	Lg	Lnu3230r Firmware	All	All	All	All
Hardware	Lg	Lnu5110r	-	All	All	All
Hardware	Lg	Lnu5110r	-	All	All	All
Operating System	Lg	Lnu5110r Firmware	All	All	All	All
Hardware	Lg	Lnu5320r	-	All	All	All
Hardware	Lg	Lnu5320r	-	All	All	All
Operating System	Lg	Lnu5320r Firmware	All	All	All	All
Hardware	Lg	Lnu7210r	-	All	All	All
Hardware	Lg	Lnu7210r	-	All	All	All
Operating System	Lg	Lnu7210r Firmware	All	All	All	All
Hardware	Lg	Lnv5110r	-	All	All	All
Hardware	Lg	Lnv5110r	-	All	All	All
Operating System	Lg	Lnv5110r Firmware	All	All	All	All
Hardware	Lg	Lnv5320r	-	All	All	All
Hardware	Lg	Lnv5320r	-	All	All	All
Operating System	Lg	Lnv5320r Firmware	All	All	All	All
Hardware	Lg	Lnv7210	-	All	All	All
Hardware	Lg	Lnv7210	-	All	All	All
Hardware	Lg	Lnv7210r	-	All	All	All
Hardware	Lg	Lnv7210r	-	All	All	All

Operating System	Lg	Lnv7210r Firmware	All	All	All	All
Operating System	Lg	Lnv7210 Firmware	All	All	All	All

## References

Reference	Source
LG Smart IP Camera 1508190 - Backup File Download - Hardware webapps Exploit	EXPLOIT-DB
GitHub - EgeBalci/LG-Smart-IP-Device-Backup-Download: Exploit for downloading backup files from LG Smart IP Devices.	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)