



CVE-2019-12111

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-12111
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-15 23:29:00 UTC
Updated	2020-09-28 20:15:00 UTC
Description	A Denial Of Service vulnerability in MiniUPnP MiniUPnPd through 2.1 exists due to a NULL pointer dereference in copyIPv6

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Miniupnp Project	Miniupnpd	All	All	All	All

References

Reference	Source	Link	Ta
USN-4542-1: MiniUPnPd vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
Security Issues Discovered in MiniUPnP VDOO	MISC	www.vdoo.com	Ex
[SECURITY] [DLA 1811-1] miniupnpd security update	MLIST	lists.debian.org	Ma
pcpserver.c: copyIPv6IfDifferent() check for NULL src argument · miniupnp/miniupnp@cb8a02a · GitHub	MISC	github.com	Pa
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501881](#) Alpine Linux Security Update for miniupnpd

© [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](#)