



CVE-2016-3179

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

Summary

CVE	CVE-2016-3179
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-24 15:59:00 UTC
Updated	2021-04-19 15:06:00 UTC
Description	The processRequest function in minissdpd.c in MiniSSDPd 1.2.20130907-3 allows local users to cause a denial of service (

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniupnp Project	Minissdpd	1.2.20130907-3	All	All	All
Application	Miniupnp Project	Minissdpd	1.2.20130907-3	All	All	All
Application	Miniupnp Project	Minissdpd	1.2.20130907-3	All	All	All

References

Reference	Source
speirofr.appspot.com/files/advisory/SPADV-2016-02.md	MISC
minissdpd.c: Initialize pointers to NULL (fix) · miniupnp/miniupnp@140ee8d · GitHub	CONFIRM
#816759 - minissdpd: CVE-2016-3178 CVE-2016-3179 - Debian Bug report logs	CONFIRM
oss-security - Re: CVE Request: The minissdpd (v 1.2.20130907-3) is affected by an improper validation of array index weakness	MLIST
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](#)