



CVE-2020-28926

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-28926 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-11-30 18:15:00 UTC |
| Updated | 2022-08-06 03:48:00 UTC |
| Description | ReadyMedia (aka MiniDLNA) before versions 1.3.0 allows remote code execution. Sending a malicious UPnP HTTP request |

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Readymedia Project | Readymedia | All | All | All | All |
| Application | Readymedia Project | Readymedia | All | All | All | All |

References

| Reference | Source |
|---|---------|
| [SECURITY] [DLA 2489-1] minidlna security update | MLIST |
| Debian -- Security Information -- DSA-4806-1 minidlna | DEBIAN |
| Rootshell Discover Remote Heap Corruption Bug Within MiniDLNA And Develop Proof Of Concept Exploit Rootshell Security | MISC |
| ReadyMedia download SourceForge.net | MISC |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501073 Alpine Linux Security Update for minidlna

505063 Alpine Linux Security Update for minidlna

750684 OpenSUSE Security Update for minidlna (openSUSE-SU-2020:2194-1)

750685 OpenSUSE Security Update for minidlna (openSUSE-SU-2020:2160-1)

© [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](#)