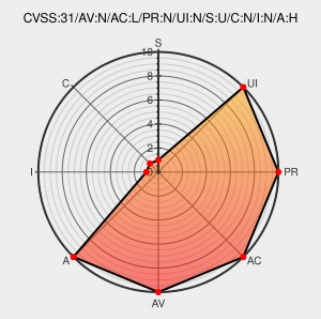
# CVE-2020-13848

Published on: 06/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:43 PM UTC

## CVE-2020-13848

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Debian Linux from Debian contain the following vulnerability:

Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c.

CVE-2020-13848 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.5 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| [security-announce] openSUSE-SU-2020:0821-1: moderate: Security update f | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2020:0821 |

| | | |
|---|---|---|
| [SECURITY] [DLA 2238-1] libupnp security update | Mailing List<br>Third Party Advisory<br>lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20200608 [SECURITY] [DLA 2238-1] libupnp security update |
| [security-announce] openSUSE-SU-2020:0805-1: moderate: Security update f | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2020:0805 |
| NULL pointer dereference in FindServiceControlURLPath · Issue #177 · pupnp/pupnp · GitHub | Third Party Advisory<br>github.com<br>text/html | MISC github.com/pupnp/pupnp/issues/177 |
| [SECURITY] [DLA 2585-1] libupnp security update | lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20210307 [SECURITY] [DLA 2585-1] libupnp security update |
| Fixes #177: NULL pointer dereference in FindServiceControlURLPath · pupnp/pupnp@c805c1d · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/pupnp/pupnp/commit/c805c1de1141cb22f74c0d94dd5664bda37398e0 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

## Related QID Numbers

501612 Alpine Linux Security Update for libupnp

690447 Free Berkeley Software Distribution (FreeBSD) Security Update for upnp (a23871f6-059b-11eb-8758-e0d55e2a8bf9)

## Known Affected Configurations (CPE V2.3)

| 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 | Libupnp Project | Libupnp | All | All | All | All |

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:libupnp_project:libupnp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred 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**