



CVE-2017-12865

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

Summary

CVE	CVE-2017-12865
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-29 16:29:00 UTC
Updated	2020-03-05 19:23:00 UTC
Description	Stack-based buffer overflow in "dnsproxy.c" in connman 1.34 and earlier allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-119

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	Intel	Connman	All	All	All	All

References

Reference	Source
1483720 – (CVE-2017-12865) CVE-2017-12865 connman: Stack-based buffer overflow in parse_response function in src/dnsproxy.c	CONF
ConnMan: Multiple vulnerabilities (GLSA 201812-02) — Gentoo security	GENT
Debian -- Security Information -- DSA-3956-1 connman	DEBI/
Buffer overflow in ConnMan Project connection manager daemon version 1.34 and earlier 01.org	CONF
connman/connman.git - Connection Manager	CONF
connman 'src/dnsproxy.c' Stack Based Buffer Overflow Vulnerability	BID
New IoT Device Vulnerability "ConnManDo"	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710252 Gentoo Linux ConnMan Multiple Vulnerabilities (GLSA 201812-02)

© [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](#)