CVE-2016-5180

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-5180
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-03 15:59:00 UTC
Updated	2023-11-07 02:33:00 UTC
Description	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to cause

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-ares	C-ares	1.0.0	All	All	All
Application	C-ares	C-ares	1.1.0	All	All	All
Application	C-ares	C-ares	1.10.0	All	All	All
Application	C-ares	C-ares	1.2.0	All	All	All
Application	C-ares	C-ares	1.2.1	All	All	All
Application	C-ares	C-ares	1.3.0	All	All	All
Application	C-ares	C-ares	1.3.1	All	All	All
Application	C-ares	C-ares	1.3.2	All	All	All
Application	C-ares	C-ares	1.4.0	All	All	All
Application	C-ares	C-ares	1.5.0	All	All	All
Application	C-ares	C-ares	1.5.1	All	All	All
Application	C-ares	C-ares	1.5.2	All	All	All
Application	C-ares	C-ares	1.5.3	All	All	All
Application	C-ares	C-ares	1.6.0	All	All	All
Application	C-ares	C-ares	1.7.0	All	All	All
Application	C-ares	C-ares	1.7.1	All	All	All
Application	C-ares	C-ares	1.7.2	All	All	All

Application	C-ares	C-ares	1.7.3	All	All	All
Application	C-ares	C-ares	1.7.4	All	All	All
Application	C-ares	C-ares	1.7.5	All	All	All
Application	C-ares	C-ares	1.8.0	All	All	All
Application	C-ares	C-ares	1.9.0	All	All	All
Application	C-ares	C-ares	1.9.1	All	All	All
Application	C-ares Project	C-ares	1.0.0	All	All	All
Application	C-ares Project	C-ares	1.1.0	All	All	All
Application	C-ares Project	C-ares	1.10.0	All	All	All
Application	C-ares Project	C-ares	1.11.0	All	All	All
Application	C-ares Project	C-ares	1.2.0	All	All	All
Application	C-ares Project	C-ares	1.2.1	All	All	All
Application	C-ares Project	C-ares	1.3.0	All	All	All
Application	C-ares Project	C-ares	1.3.1	All	All	All
Application	C-ares Project	C-ares	1.3.2	All	All	All
Application	C-ares Project	C-ares	1.4.0	All	All	All
Application	C-ares Project	C-ares	1.5.0	All	All	All
Application	C-ares Project	C-ares	1.5.1	All	All	All
Application	C-ares Project	C-ares	1.5.2	All	All	All
Application	C-ares Project	C-ares	1.5.3	All	All	All
Application	C-ares Project	C-ares	1.6.0	All	All	All
Application	C-ares Project	C-ares	1.7.0	All	All	All
Application	C-ares Project	C-ares	1.7.1	All	All	All
Application	C-ares Project	C-ares	1.7.2	All	All	All
Application	C-ares Project	C-ares	1.7.3	All	All	All
Application	C-ares Project	C-ares	1.7.4	All	All	All
Application	C-ares Project	C-ares	1.7.5	All	All	All
Application	C-ares Project	C-ares	1.8.0	All	All	All
Application	C-ares Project	C-ares	1.9.0	All	All	All
Application	C-ares Project	C-ares	1.9.1	All	All	All
Application	C-ares Project	C-ares	1.0.0	All	All	All
Application	C-ares Project	C-ares	1.1.0	All	All	All
Application	C-ares Project	C-ares	1.10.0	All	All	All
Application	C-ares Project	C-ares	1.11.0	All	All	All
Application	C-ares Project	C-ares	1.2.0	All	All	All

Application	C-ares Project	C-ares	1.2.1	All	All	All
Application	C-ares Project	C-ares	1.3.0	All	All	All
Application	C-ares Project	C-ares	1.3.1	All	All	All
Application	C-ares Project	C-ares	1.3.2	All	All	All
Application	C-ares Project	C-ares	1.4.0	All	All	All
Application	C-ares Project	C-ares	1.5.0	All	All	All
Application	C-ares Project	C-ares	1.5.1	All	All	All
Application	C-ares Project	C-ares	1.5.2	All	All	All
Application	C-ares Project	C-ares	1.5.3	All	All	All
Application	C-ares Project	C-ares	1.6.0	All	All	All
Application	C-ares Project	C-ares	1.7.0	All	All	All
Application	C-ares Project	C-ares	1.7.1	All	All	All
Application	C-ares Project	C-ares	1.7.2	All	All	All
Application	C-ares Project	C-ares	1.7.3	All	All	All
Application	C-ares Project	C-ares	1.7.4	All	All	All
Application	C-ares Project	C-ares	1.7.5	All	All	All
Application	C-ares Project	C-ares	1.8.0	All	All	All
Application	C-ares Project	C-ares	1.9.0	All	All	All
Application	C-ares Project	C-ares	1.9.1	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Nodejs	Node.js	All	All	All	All

References

Reference	Source	Link	Tags
USN-3143-1: c-ares vulnerability | Ubuntu	UBUNTU	www.ubuntu.com	
Chrome Releases: Stable Channel Update for Chrome OS	CONFIRM	googlechromereleases.blogspot.in	Third Party A
C-ares CVE-2016-5180 Out of Bounds Write Denial of Service Vulnerability		www.securityfocus.com	
Debian -- Security Information -- DSA-3682-1 c-ares	DEBIAN	www.debian.org	Third Party A
Red Hat Customer Portal		rhn.redhat.com	
Android Security Bulletin—January 2017 | Android Open Source Project		source.android.com	
c-ares: Heap-based buffer overflow (GLSA 201701-28) — Gentoo security		security.gentoo.org	

c-ares.haxx.se/CVE-2016-5180.patch		c-ares.haxx.se	
ares_create_query single byte out of buffer write		c-ares.haxx.se	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710452 Gentoo Linux c-ares Heap-based buffer overflow Vulnerability (GLSA 201701-28)