CVE-2017-8816

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-8816
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-29 18:29:00 UTC
Updated	2026-04-15 21:16:58 UTC
Description	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of s

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.004540000 probability, percentile 0.638470000 (date 2026-04-15)

Problem Types: CWE-190 | integer overflow | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

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	9.0	All	All	All
Application	Haxx	Curl	All	All	All	All
Application	Haxx	Libcurl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Curl And Libcurl Before 7.57.0	affected curl and libcurl before 7.57.0	Not specified

References

Reference
Debian -- Security Information -- DSA-4051-1 curl
cURL/libcURL CVE-2017-8816 Buffer Overflow Vulnerability
Red Hat Customer Portal
CLD-161 Details
Apple macOS/OS X Multiple Flaws Let Remote Users Bypass Security and Obtain Potentially Sensitive Information and Let Local Users Obtai
curl - NTLM buffer overflow via integer overflow
libcurl NTLM Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker
cURL: Multiple vulnerabilities (GLSA 201712-04) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500121 Alpine Linux Security Update for curl

503776 Alpine Linux Security Update for curl

710458 Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201712-04)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report