CVE-2017-1000101

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

Summary

CVE	CVE-2017-1000101
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-05 01:29:04 UTC
Updated	2026-04-16 14:16:10 UTC
Description	curl supports "globbing" of URLs, in which a user can pass a numerical range to have the tool iterate over those numbers to

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.007630000 probability, percentile 0.734140000 (date 2026-04-21)

Problem Types: CWE-119 | n/a | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
3.0	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haxx	Curl	7.35.0	All	All	All
Application	Haxx	Curl	7.36.0	All	All	All
Application	Haxx	Curl	7.37.0	All	All	All
Application	Haxx	Curl	7.37.1	All	All	All
Application	Haxx	Curl	7.38.0	All	All	All
Application	Haxx	Curl	7.39.0	All	All	All
Application	Haxx	Curl	7.4.1	All	All	All
Application	Haxx	Curl	7.40.0	All	All	All
Application	Haxx	Curl	7.41.0	All	All	All
Application	Haxx	Curl	7.42.0	All	All	All
Application	Haxx	Curl	7.42.1	All	All	All
Application	Haxx	Curl	7.43.0	All	All	All
Application	Haxx	Curl	7.44.0	All	All	All
Application	Haxx	Curl	7.45.0	All	All	All
Application	Haxx	Curl	7.46.0	All	All	All
Application	Haxx	Curl	7.47.0	All	All	All
Application	Haxx	Curl	7.47.1	All	All	All
Application	Haxx	Curl	7.48.0	All	All	All
Application	Haxx	Curl	7.49.0	All	All	All
Application	Haxx	Curl	7.49.1	All	All	All
Application	Haxx	Curl	7.50.0	All	All	All
Application	Haxx	Curl	7.50.1	All	All	All
Application	Haxx	Curl	7.50.2	All	All	All
Application	Haxx	Curl	7.50.3	All	All	All
Application	Haxx	Curl	7.51.0	All	All	All
Application	Haxx	Curl	7.52.0	All	All	All
Application	Haxx	Curl	7.52.1	All	All	All
Application	Haxx	Curl	7.53.0	All	All	All
Application	Haxx	Curl	7.53.1	All	All	All
Application	Haxx	Curl	7.54.0	All	All	All
Application	Haxx	Curl	7.54.1	All	All	All
Application	Haxx	Curl	7.55.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
curl - URL globbing out of bounds read
Debian -- Security Information -- DSA-3992-1 curl
Red Hat Customer Portal
cURL: Multiple vulnerabilities (GLSA 201709-14) — Gentoo Security
cURL URL Globbing Flaw Lets Local Users View Portions of System Memory on the Target System - SecurityTracker
Malformed Request
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 500119 Alpine Linux Security Update for curl
- 503774 Alpine Linux Security Update for curl
- 710401 Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201709-14)

Free CVE JSON API cve.report/api

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