



# CVE-2017-1000101

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-1000101
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-05 01:29:04 UTC
<b>Updated</b>	2026-04-16 14:16:10 UTC
<b>Description</b>	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)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)