



CVE-2017-1000257

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

Summary

CVE	CVE-2017-1000257
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-31 21:29:00 UTC
Updated	2026-04-15 21:16:57 UTC
Description	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the da

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ADP

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

EPSS: 0.010010000 probability, percentile 0.770290000 (date 2026-04-15)

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	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.0	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
2.0	nvd@nist.gov	Primary	6.4		AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:N/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	Libcurl	All	All	All	All

Vendor Declared Affected Products

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

References

Reference

[Red Hat Customer Portal](#)

[cURL Buffer Overread in Processing IMAP FETCH Response Data Lets Remote Users Deny Service or Obtain Potentially Sensitive Information](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Debian -- Security Information -- DSA-4007-1 curl](#)

[curl - IMAP FETCH response out of bounds read](#)

[cURL/libcURL CVE-2017-1000257 Buffer Overflow Vulnerability](#)

[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

[378161](#) Virtuozzo Linux Security Update for libcurl (VZLSA-2017:3263)

[500120](#) Alpine Linux Security Update for curl

[503775](#) Alpine Linux Security Update for curl

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

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