



CVE-2010-0734

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

Summary

CVE	CVE-2010-0734
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-19 19:30:00 UTC
Updated	2018-10-10 19:53:00 UTC
Description	content_encoding.c in libcurl 7.10.5 through 7.19.7, when zlib is enabled, does not properly restrict the amount of callback c

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Curl	Libcurl	7.10.5	All	All	All
Application	Curl	Libcurl	7.10.6	All	All	All
Application	Curl	Libcurl	7.10.7	All	All	All
Application	Curl	Libcurl	7.10.8	All	All	All
Application	Curl	Libcurl	7.11.0	All	All	All
Application	Curl	Libcurl	7.11.1	All	All	All
Application	Curl	Libcurl	7.11.2	All	All	All
Application	Curl	Libcurl	7.12	All	All	All
Application	Curl	Libcurl	7.12.0	All	All	All
Application	Curl	Libcurl	7.12.1	All	All	All
Application	Curl	Libcurl	7.12.2	All	All	All
Application	Curl	Libcurl	7.12.3	All	All	All
Application	Curl	Libcurl	7.13	All	All	All
Application	Curl	Libcurl	7.13.1	All	All	All
Application	Curl	Libcurl	7.13.2	All	All	All
Application	Curl	Libcurl	7.14	All	All	All
Application	Curl	Libcurl	7.14.1	All	All	All

Application	Curl	Libcurl	7.15	All	All	All
Application	Curl	Libcurl	7.15.1	All	All	All
Application	Curl	Libcurl	7.15.2	All	All	All
Application	Curl	Libcurl	7.15.3	All	All	All
Application	Curl	Libcurl	7.16.3	All	All	All
Application	Curl	Libcurl	7.17.0	All	All	All
Application	Curl	Libcurl	7.17.1	All	All	All
Application	Curl	Libcurl	7.18.0	All	All	All
Application	Curl	Libcurl	7.18.1	All	All	All
Application	Curl	Libcurl	7.18.2	All	All	All
Application	Curl	Libcurl	7.19.0	All	All	All
Application	Curl	Libcurl	7.19.1	All	All	All
Application	Curl	Libcurl	7.19.2	All	All	All
Application	Curl	Libcurl	7.19.3	All	All	All
Application	Curl	Libcurl	7.19.4	All	All	All
Application	Curl	Libcurl	7.19.5	All	All	All
Application	Curl	Libcurl	7.19.6	All	All	All
Application	Curl	Libcurl	7.19.7	All	All	All
Application	Curl	Libcurl	7.10.5	All	All	All
Application	Curl	Libcurl	7.10.6	All	All	All
Application	Curl	Libcurl	7.10.7	All	All	All
Application	Curl	Libcurl	7.10.8	All	All	All
Application	Curl	Libcurl	7.11.0	All	All	All
Application	Curl	Libcurl	7.11.1	All	All	All
Application	Curl	Libcurl	7.11.2	All	All	All
Application	Curl	Libcurl	7.12	All	All	All
Application	Curl	Libcurl	7.12.0	All	All	All
Application	Curl	Libcurl	7.12.1	All	All	All
Application	Curl	Libcurl	7.12.2	All	All	All
Application	Curl	Libcurl	7.12.3	All	All	All
Application	Curl	Libcurl	7.13	All	All	All
Application	Curl	Libcurl	7.13.1	All	All	All
Application	Curl	Libcurl	7.13.2	All	All	All
Application	Curl	Libcurl	7.14	All	All	All
Application	Curl	Libcurl	7.14.1	All	All	All

Application	Curl	Libcurl	7.15	All	All	All
Application	Curl	Libcurl	7.15.1	All	All	All
Application	Curl	Libcurl	7.15.2	All	All	All
Application	Curl	Libcurl	7.15.3	All	All	All
Application	Curl	Libcurl	7.16.3	All	All	All
Application	Curl	Libcurl	7.17.0	All	All	All
Application	Curl	Libcurl	7.17.1	All	All	All
Application	Curl	Libcurl	7.18.0	All	All	All
Application	Curl	Libcurl	7.18.1	All	All	All
Application	Curl	Libcurl	7.18.2	All	All	All
Application	Curl	Libcurl	7.19.0	All	All	All
Application	Curl	Libcurl	7.19.1	All	All	All
Application	Curl	Libcurl	7.19.2	All	All	All
Application	Curl	Libcurl	7.19.3	All	All	All
Application	Curl	Libcurl	7.19.4	All	All	All
Application	Curl	Libcurl	7.19.5	All	All	All
Application	Curl	Libcurl	7.19.6	All	All	All
Application	Curl	Libcurl	7.19.7	All	All	All

References

Reference	Source
Support	RED
About the security content of Security Update 2010-004 / Mac OS X v10.6.4	COF
curl.haxx.se/libcurl-contentencoding.patch	COF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
curl - Security Problems	COF
Gentoo Linux Documentation -- cURL: Multiple vulnerabilities	GEN
USN-1158-1: curl vulnerabilities Ubuntu	UBL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
SecurityFocus	BUK
Debian update for curl - Secunia.com	SEC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
[SECURITY] Fedora 11 Update: curl-7.19.7-5.fc11	FED
Security Advisory SA48256 - Gentoo update for curl - Secunia	SEC
VMSA-2011-0003	COF
APPLE-SA-2010-06-15-1 Security Update 2010-004 / Mac OS X v10.6.4	APP

Fedora update for curl - Advisories - Community	SEC
oss-security - Re: CVE Request -- cURL/libCURL 7.20.0	MLI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
oss-security - CVE Request -- cURL/libCURL 7.20.0	MLI
Avaya Products curl Excessive Data Length in Callback Function - Advisories - Community	SEC
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Community	SEC
Bug 563220 – CVE-2010-0734 curl: zlib-compression causes curl to pass more than CURL_MAX_WRITE_SIZE bytes to write callback	COI
[SECURITY] Fedora 12 Update: curl-7.19.7-7.fc12	FED
cURL - Security Advisory (February 9, 2010)	COI
Repository / Oval Repository	OVA
Ubuntu update for curl - Secunia.com	SEC
Advisories Mandriva	MAI
ASA-2010-126 (RHSA-2010-0329)	COI
Fedora update for curl - Secunia.com	SEC
oss-security - Re: CVE Request -- cURL/libCURL 7.20.0	MLI
Advisories:rPSA-2010-0072 - rPath Wiki	COI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
SecurityFocus	BUK
Debian -- Security Information -- DSA-2023-1 curl	DEE
Repository / Oval Repository	OVA
CVE Program record	CVE
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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