CVE-2009-2417

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

Summary

CVE	CVE-2009-2417
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-14 15:16:27 UTC
Updated	2026-04-23 00:35:47 UTC
Description	lib/ssluse.c in cURL and libcurl 7.4 through 7.19.5, when OpenSSL is used, does not properly handle a '\0' character in a dc

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

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
Application	Curl	Libcurl	7.10	All	All	All

Application	Curl	Libcurl	7.10.1	All	All	All
Application	Curl	Libcurl	7.10.2	All	All	All
Application	Curl	Libcurl	7.10.3	All	All	All
Application	Curl	Libcurl	7.10.4	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	7.4	All	All	All
Application	Curl	Libcurl	7.4.1	All	All	All
Application	Curl	Libcurl	7.4.2	All	All	All
Application	Curl	Libcurl	7.5	All	All	All
Application	Curl	Libcurl	7.5.1	All	All	All
Application	Curl	Libcurl	7.5.2	All	All	All
Application	Curl	Libcurl	7.6	All	All	All
Application	Curl	Libcurl	7.6.1	All	All	All
Application	Curl	Libcurl	7.7	All	All	All
Application	Curl	Libcurl	7.7.1	All	All	All
Application	Curl	Libcurl	7.7.2	All	All	All
Application	Curl	Libcurl	7.7.3	All	All	All
Application	Curl	Libcurl	7.8	All	All	All
Application	Curl	Libcurl	7.8.1	All	All	All
Application	Curl	Libcurl	7.9	All	All	All
Application	Curl	Libcurl	7.9.1	All	All	All
Application	Curl	Libcurl	7.9.2	All	All	All
Application	Curl	Libcurl	7.9.3	All	All	All
Application	Curl	Libcurl	7.9.5	All	All	All
Application	Curl	Libcurl	7.9.6	All	All	All
Application	Curl	Libcurl	7.9.7	All	All	All
Application	Curl	Libcurl	7.9.8	All	All	All
Application	Libcurl	Libcurl	7.12	All	All	All
Application	Libcurl	Libcurl	7.12.1	All	All	All
Application	Libcurl	Libcurl	7.12.2	All	All	All
Application	Libcurl	Libcurl	7.12.3	All	All	All
Application	Libcurl	Libcurl	7.13	All	All	All
Application	Libcurl	Libcurl	7.13.1	All	All	All
Application	Libcurl	Libcurl	7.13.2	All	All	All
Application	Libcurl	Libcurl	7.14	All	All	All
Application	Libcurl	Libcurl	7.14.1	All	All	All
Application	Libcurl	Libcurl	7.15	All	All	All
Application	Libcurl	Libcurl	7.15.1	All	All	All
Application	Libcurl	Libcurl	7.15.2	All	All	All

Application	Libcurl	Libcurl	7.15.3	All	All	All
Application	Libcurl	Libcurl	7.16.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b
curl: page not found	af854a3a-2127-422b
IBM X-Force Exchange	af854a3a-2127-422b
Repository / Oval Repository	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.19.5-CVE-2009-2417.patch	af854a3a-2127-422b
rPath update for curl - Secunia.com	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.16.4-CVE-2009-2417.patch	af854a3a-2127-422b
USN-1158-1: curl vulnerabilities | Ubuntu	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.11.0-CVE-2009-2417.patch	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.15.1-CVE-2009-2417.patch	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.12.1-CVE-2009-2417.patch	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.15.5-CVE-2009-2417.patch	af854a3a-2127-422b
cURL OpenSSL NULL Character Spoofing Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b
Repository / Oval Repository	af854a3a-2127-422b
Shibboleth - InCommon	af854a3a-2127-422b
SecurityFocus	af854a3a-2127-422b
Webmail - OVH	af854a3a-2127-422b
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-422b
wiki.rpath.com/Advisories:rPSA-2009-0124	af854a3a-2127-422b
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-422b
Ubuntu update for curl - Secunia.com	af854a3a-2127-422b
VMSA-2009-0016.1	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.19.0-CVE-2009-2417.patch	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.10.6-CVE-2009-2417.patch	af854a3a-2127-422b
SecurityFocus	af854a3a-2127-422b
curl.haxx.se/CVE-2009-2417/curl-7.18.1-CVE-2009-2417.patch	af854a3a-2127-422b

cURL / libcURL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability	af854a3a-2127-422b
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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