CVE-2009-0037

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

Summary

CVE	CVE-2009-0037
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-05 02:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The redirect implementation in curl and libcurl 5.11 through 7.19.3, when CURLOPT_FOLLOWLOCATION is enabled, acce

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Curl	Curl	5.11	All	All	All

Application	Curl	Curl	6.0	All	All	All
Application	Curl	Curl	6.1beta	All	All	All
Application	Curl	Curl	6.2	All	All	All
Application	Curl	Curl	6.3	All	All	All
Application	Curl	Curl	6.3.1	All	All	All
Application	Curl	Curl	6.4	All	All	All
Application	Curl	Curl	6.5	All	All	All
Application	Curl	Curl	6.5.1	All	All	All
Application	Curl	Curl	6.5.2	All	All	All
Application	Curl	Curl	7.1	All	All	All
Application	Curl	Curl	7.1.1	All	All	All
Application	Curl	Curl	7.10	All	All	All
Application	Curl	Curl	7.10.1	All	All	All
Application	Curl	Curl	7.10.2	All	All	All
Application	Curl	Curl	7.10.3	All	All	All
Application	Curl	Curl	7.10.4	All	All	All
Application	Curl	Curl	7.10.5	All	All	All
Application	Curl	Curl	7.10.6	All	All	All
Application	Curl	Curl	7.10.7	All	All	All
Application	Curl	Curl	7.10.8	All	All	All
Application	Curl	Curl	7.11.1	All	All	All
Application	Curl	Curl	7.12	All	All	All
Application	Curl	Curl	7.12.1	All	All	All
Application	Curl	Curl	7.12.2	All	All	All
Application	Curl	Curl	7.13	All	All	All
Application	Curl	Curl	7.13.2	All	All	All
Application	Curl	Curl	7.14	All	All	All
Application	Curl	Curl	7.14.1	All	All	All
Application	Curl	Curl	7.15	All	All	All
Application	Curl	Curl	7.15.1	All	All	All
Application	Curl	Curl	7.15.3	All	All	All
Application	Curl	Curl	7.16.3	All	All	All
Application	Curl	Curl	7.16.4	All	All	All
Application	Curl	Curl	7.17	All	All	All
Application	Curl	Curl	7.18	All	All	All
Application	Curl	Curl	7.19.3	All	All	All

Application	Curl	Curl	7.2	All	All	All
Application	Curl	Curl	7.2.1	All	All	All
Application	Curl	Curl	7.3	All	All	All
Application	Curl	Curl	7.4	All	All	All
Application	Curl	Curl	7.4.1	All	All	All
Application	Curl	Curl	7.4.2	All	All	All
Application	Curl	Curl	7.5	All	All	All
Application	Curl	Curl	7.5.1	All	All	All
Application	Curl	Curl	7.5.2	All	All	All
Application	Curl	Curl	7.6	All	All	All
Application	Curl	Curl	7.6.1	All	All	All
Application	Curl	Curl	7.7	All	All	All
Application	Curl	Curl	7.7.1	All	All	All
Application	Curl	Curl	7.7.2	All	All	All
Application	Curl	Curl	7.7.3	All	All	All
Application	Curl	Curl	7.8	All	All	All
Application	Curl	Curl	7.8.1	All	All	All
Application	Curl	Curl	7.8.2	All	All	All
Application	Curl	Curl	7.9	All	All	All
Application	Curl	Curl	7.9.1	All	All	All
Application	Curl	Curl	7.9.2	All	All	All
Application	Curl	Curl	7.9.3	All	All	All
Application	Curl	Curl	7.9.4	All	All	All
Application	Curl	Curl	7.9.5	All	All	All
Application	Curl	Curl	7.9.6	All	All	All
Application	Curl	Curl	7.9.7	All	All	All
Application	Curl	Curl	7.9.8	All	All	All
Application	Curl	Libcurl	5.11	All	All	All
Application	Curl	Libcurl	7.12	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	7.19.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
USN-726-1: curl vulnerability | Ubuntu	af854a3a-2127-422b-91
cURL/libcURL HTTP 'Location:' Redirect Security Bypass Vulnerability	af854a3a-2127-422b-91
Support	af854a3a-2127-422b-91
SecurityFocus	af854a3a-2127-422b-91
www.withdk.com/archives/Libcurl_arbitrary_file_access.pdf	af854a3a-2127-422b-91
IBM X-Force Exchange	af854a3a-2127-422b-91
Repository / Oval Repository	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-1738-1 curl	af854a3a-2127-422b-91
SUSE Update for Multiple Packages - Advisories - Community	af854a3a-2127-422b-91
curl: page not found	af854a3a-2127-422b-91
rPath update for curl - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91
With DK » Blog Archive » cURL/LibcURL Redirect Arbitrary File Access	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Slackware update for curl - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91
[Security-announce] VMSA-2009-0009 ESX Service Console updates for udev, sudo, and curl	af854a3a-2127-422b-91
cURL/libcurl HTTP Redirect Processing May Let Remote Users Access Files - SecurityTracker	af854a3a-2127-422b-91
VMware ESX Server update for udev, sudo, and curl - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91
Debian update for curl - Secunia.com	af854a3a-2127-422b-91
Repository / Oval Repository	af854a3a-2127-422b-91
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-422b-91
Webmail - OVH	af854a3a-2127-422b-91

VMSA-2009-0009	af854a3a-2127-422b-91
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	af854a3a-2127-422b-91
Gentoo update for curl - Secunia.com	af854a3a-2127-422b-91
Advisories:rPSA-2009-0042 - rPath Wiki	af854a3a-2127-422b-91
The Slackware Linux Project: Slackware Security Advisories	af854a3a-2127-422b-91
Red Hat update for curl - Secunia.com	af854a3a-2127-422b-91
cURL/libcURL "Location:" Redirect URLs Security Bypass - Advisories - Community	af854a3a-2127-422b-91
SecurityFocus	af854a3a-2127-422b-91
cURL - Security Advisory (March 3, 2009)	af854a3a-2127-422b-91
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:006	af854a3a-2127-422b-91
Gentoo Linux Documentation -- cURL: Arbitrary file access	af854a3a-2127-422b-91
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.