



CVE-2005-3185

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

Summary

CVE	CVE-2005-3185
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-13 22:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in the ntlm_output function in http-ntlm.c for (1) wget 1.10, (2) curl 7.13.2, and (3) libcurl 7.13.2

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-119 | 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	Curl	7.13.2	All	All	All

Application	Libcurl	Libcurl	7.13.2	All	All	All
Application	Wget	Wget	1.10	All	All	All

Vendor Declared Affected Products

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

References

Reference

Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities

Repository / Oval Repository

Secunia - Advisories - Gentoo update for curl

<ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.10/SCOSA-2006.10.txt>

Secunia - Advisories - Red Hat update for curl

Accenture | Let there be change

About Security Update 2005-009

Advisories - Mandriva

[SECURITY] Fedora Core 4 Update: curl-7.13.1-4.fc4

www.osvdb.org/20011

SecurityTracker.com Archives - cURL/libcurl Buffer Overflow in Processing NTLM Authentication Values May Let Remote Users Execute Arbit

Secunia - Advisories - cURL/libcURL NTLM Username Handling Buffer Overflow Vulnerability

Secunia - Advisories - SUSE update for curl/wget

Secunia - Advisories - Red Hat update for wget

Security Announcement

Secunia - Advisories - Slackware updates for curl/wget

IBM X-Force Exchange

Secunia - Advisories - Mandrake update for curl

Secunia - Advisories - Fedora update for wget

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian update for curl - Secunia Advisories - Vulnerability Intelligence - Secunia.com

TLSA-2005-0059 - multi

Fedora update for curl - Advisories - Secunia

SecurityTracker.com Archives - wget Buffer Overflow in Processing NTLM Authentication Values May Let Remote Users Execute Arbitrary Co

Gentoo Linux Documentation -- cURL: NTLM username stack overflow

Debian -- Security Information -- DSA-919-2 curl

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Secunia - Advisories - Ubuntu update for libcurl2/libcurl2

Secunia - Advisories - Ubuntu update for libcurl/libcurl3

[SECURITY] Fedora Core 3 Update: curl-7.12.3-4.fc3

Webmail - OVH

Support

SecurityReason - Multiple Vendor wget/curl NTLM Username Buffer Overflow Vulnerability

Multiple Vendor WGet/Curl NTLM Username Buffer Overflow Vulnerability

RETIRED: Apple Mac OS X Security Update 2005-009 Multiple Vulnerabilities

Secunia - Advisories - SCO OpenServer Updates for Multiple Packages

Support

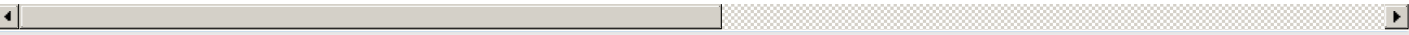
USN-205-1: Curl and wget vulnerabilities | Ubuntu security notices

The Slackware Linux Project: Slackware Security Advisories

Secunia - Advisories - wget NTLM Username Handling Buffer Overflow Vulnerability

CVE Program record

NVD vulnerability detail



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](#)