# CVE Detail – CVE-2005-0490

Multiple stack-based buffer overflows in libcURL and cURL 7.12.1, and possibly other versions, allow remote malicious web servers to execute arbitrary code via base64 encoded replies that exceed the intended buffer lengths when decoded, which is not properly handled by (1) the Curl\_input\_ntlm function in http\_ntlm.c during NTLM authentication or (2) the Curl\_krb\_kauth and krb4\_auth functions in krb4.c during Kerberos authentication.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.84928

## CVSS Scoring

CVSS v3.1 Score: 8.8

Severity: HIGH

## Mapped CWE(s)

* CWE-131: Incorrect Calculation of Buffer Size

## CAPEC(s)

* CAPEC-100: Overflow Buffers
* CAPEC-47: Buffer Overflow via Parameter Expansion

## Affected Products

* cpe:2.3:a:haxx:curl:7.12.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:haxx:libcurl:7.12.1:\*:\*:\*:\*:\*:\*:\*