



leancrypto: Integer truncation in X.509 name parser enables certificate identity impersonation

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

Summary

CVE CVE-2026-34610

State PUBLISHED

Assigner GitHub_M

Source Priority CVE Program / NVD first with legacy fallback

Published 2026-04-02 18:16:32 UTC

Updated 2026-04-02 18:16:32 UTC

Description The leancrypto library is a cryptographic library that exclusively contains only PQC-resistant cryptographic algorithms. Prior

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from security-advisories@github.com

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Problem Types: CWE-681 | CWE-681 CWE-681: Incorrect Conversion between Numeric Types

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SmuellerDD	Leancrypto	affected < 1.7.1	Not specified

References

Reference	Source	Link	Tag
github.com/smuellerDD/leancrypto/releases/tag/v1.7.1	security-advisories@github.com	github.com	
github.com/smuellerDD/leancrypto/security/advisories/GHSA-636g-jxv4-v4gr	security-advisories@github.com	github.com	
github.com/smuellerDD/leancrypto/commit/5cdcbe12bd6c3d6e87e969972a580b44...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)