# Botan: Case-Insensitive CN Values Bypass DNS excludedSubtrees Name Constraints (RFC 5280 Violation)

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-32884 |
| **State** | PUBLISHED |
| **Assigner** | GitHub_M |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-03-30 21:17:10 UTC |
| **Updated** | 2026-04-01 14:24:02 UTC |
| **Description** | Botan is a C++ cryptography library. Prior to version 3.11.0, during processing of an X.509 certificate path using name cons |

## 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

**EPSS:** 0.000160000 probability, percentile 0.035680000 (date 2026-04-01)

**Problem Types:** CWE-295 | CWE-295 CWE-295: Improper Certificate Validation

| 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

ntegrity

High

vailability

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 | Randombit | Botan | affected < 3.11.0 | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| github.com/randombit/botan/security/advisories/GHSA-7c3g-7763-ggj5 | security-advisories@github.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysi |

No vendor comments have been submitted for this CVE.

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