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

Moderate **randombit** published **GHSA-7c3g-7763-ggj5** last month

Package

botan

Affected versions

<= 3.10.0

Patched versions

3.11.0

Description

Summary

During processing of an X.509 certificate path using name constraints which restrict the set of allowable DNS names, if no subject alternative name is defined in the end-entity certificate Botan would check that the CN was allowed by the DNS name constraints, even though this check is technically not required by RFC 5280. However this check failed to account for the possibility of a mixed-case CN. Thus a certificate with `CN=Sub.EVIL.COM` and no subject alternative name would bypasses an `excludedSubtrees` constraint for `evil.com` because the comparison is case-sensitive.

Impact

A certificate with mixed-case CN and no SANs can bypass `excludedSubtrees` name constraints. An attacker holding such a certificate (e.g., issued by a misconfigured or compromised sub-CA) can present it to clients using Botan, and the excluded domain constraint will not be enforced. This is primarily relevant in enterprise/government PKI environments that use `nameConstraints` to limit CA issuance scope (US FPKI, EU eIDAS, CAB Forum BR Section 7.1.5 technically constrained sub-CAs).

- **CWE-295**: Improper Certificate Validation
- **CWE-178**: Improper Handling of Case Sensitivity

Severity

Moderate 5.9 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-32884

Weaknesses

▶ CWE-295

Credits

 **HarutoKimura** Reporter