

randombit / botan Public

[Code](#) [Issues](#) [225](#) [Pull requests](#) [64](#) [Discussions](#) [Actions](#) [Wiki](#)

Missing OCSP Response Signature Verification Allows MitM Certificate Revocation Bypass

Moderate randombit published [GHSA-9j2j-hqmc-hf5x](#) last week

Package

botan

Affected versions

Between 3.0.0 and 3.10.0

Patched versions

3.11.0

Description

Summary

During X509 path validation, OCSP responses were checked for an appropriate status code, but critically omitted verifying the signature of the OCSP response itself.

This bug was introduced in version 3.0.0; OCSP handling in 2.x is not affected.

Impact

A MitM attacker positioned between a Botan-based client and an OCSP responder can tamper with OCSP response bodies without detection. OCSP uses plain HTTP in most deployments, making MitM via DNS hijack, BGP hijack, or rogue network AP realistic.

- **CWE-347**: Improper Verification of Cryptographic Signature
- **CWE-299**: Improper Check for Certificate Revocation

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-2026-32883

Weaknesses

▶ CWE-347

Credits



HarutoKimura

Reporter