Certificate authentication bypass due to trust anchor confusion

Critical **randombit** published **GHSA-v782-6fq4-q827** 2 days ago

Package

botan

Affected versions

3.11.0

Patched versions

3.11.1

Description

Impact

Botan 3.11.0 contains a bug which allows an attacker to bypass X509 certificate verification.

Description

The function `Certificate_Store::certificate_known` had a misleading name; it would return true if any certificate in the store had a DN (and subject key identifier, if set) matching that of the argument. It did not check that the cert it found and the cert it was passed were actually the same certificate.

In 3.11.0 an extension of path validation logic was made which assumed that `certificate_known` only returned true if the certificates were in fact identical. The impact is that if an end entity certificate is presented, and its DN (and subject key identifier, if set) match that of any trusted root, the end entity certificate is accepted immediately as if it itself were a trusted root.

Credit

Nicholas Carlini with Claude, Anthropic

Severity

Critical

CVE ID

CVE-2026-34580

Weaknesses

▶ CWE-295