Heap Buffer Over-read (up to 31 bytes) in SM2 Decryption via Undersized C3 Hash Field

High **randombit** published **GHSA-7jj6-4r42-w9h6** last month

Package

botan

Affected versions

2.3.0 - 3.10.0

Patched versions

3.11.0

Description

Summary

During SM2 decryption, the code that checked the authentication code value (`C3`) failed to check that the encoded value was of the expected length prior to comparison. An invalid ciphertext can cause a heap over-read of up to 31 bytes, resulting in a crash or potentially other undefined behavior.

Impact

Any application using Botan's SM2 encryption for message decryption is affected. An attacker can send a crafted SM2 ciphertext that causes a 31-byte heap buffer over-read, likely crashing the process (DoS). SM2 is used in Chinese standards-compliant TLS (TLCP), payment systems, and enterprise applications where servers process attacker-controlled ciphertexts over the network.

- **Availability: High**: Process crash or other undefined behavior
- **CWE-125**: Out-of-bounds Read

Severity

High 8.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-32877

Weaknesses

▶ CWE-125

Credits

HarutoKimura Reporter