



Botan: Heap Buffer Over-read in SM2 Decryption via Undersized C3 Hash Field

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2026-32877
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 21:17:09 UTC
Updated	2026-04-01 14:24:02 UTC
Description	Botan is a C++ cryptography library. From version 2.3.0 to before version 3.11.0, during SM2 decryption, the code that che

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from security-advisories@github.com

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

EPSS: 0.000450000 probability, percentile 0.137570000 (date 2026-04-01)

Problem Types: CWE-125 | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
3.1	CNA	DECLARED	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Randombit	Botan	affected >= 2.3.0, < 3.11.0	Not specified

References

Reference	Source	Link	Tags
github.com/randombit/botan/security/advisories/GHSA-7jj6-4r42-w9h6	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)