



# CVE-2018-20187

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

## Summary

<b>CVE</b>	CVE-2018-20187
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-08 19:29:00 UTC
<b>Updated</b>	2019-03-12 20:39:00 UTC
<b>Description</b>	A side-channel issue was discovered in Botan before 2.9.0. An attacker capable of precisely measuring the time taken for E

## Risk And Classification

**Problem Types:** CWE-320

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Botan Project</a>	Botan	All	All	All	All
Application	<a href="#">Botan Project</a>	Botan	All	All	All	All

## References

### Reference

- Security Advisories — Botan
- GitHub - crocs-muni/ECTester: Tests support and behavior of elliptic curve cryptography implementations on JavaCards (TYPE\_EC\_FP and T
- Release Notes — Botan
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">500074</a> Alpine Linux Security Update for botan
<a href="#">503750</a> Alpine Linux Security Update for botan

2025-05-08 10:00:00 UTC | CVE-2018-20187 | CVE-2018-20187 | CVE-2018-20187 | CVE-2018-20187 | CVE-2018-20187 | CVE-2018-20187 | CVE-2018-20187

© [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](#)**