CVE-2018-20187

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-20187
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-08 19:29:00 UTC
Updated	2019-03-12 20:39:00 UTC
Description	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	Botan Project	Botan	All	All	All	All
Application	Botan Project	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

500074 Alpine Linux Security Update for botan

503750 Alpine Linux Security Update for botan

690251 Free Berkeley Software Distribution (FreeBSD) Security Update for botan2 (d8e7e854-171a-11e9-bef6-6805ca21a271)