CVE-2018-12435

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-12435
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-15 02:29:00 UTC
Updated	2018-08-22 19:57:00 UTC
Description	Botan 2.5.0 through 2.6.0 before 2.7.0 allows a memory-cache side-channel attack on ECDSA signatures, aka the Return C

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Botan Project	Botan	All	All	All	All

References

Reference	Source	Link	Tags
Address DSA/ECDSA side channel · randombit/botan@48fc8df · GitHub	CONFIRM	github.com	Patch, Third Party
www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-numbe...	MISC	www.nccgroup.trust	Exploit, Third Part
Security Advisories — Botan	CONFIRM	botan.randombit.net	Third Party Advisc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500073 Alpine Linux Security Update for botan

503749 Alpine Linux Security Update for botan