



CVE-2019-14318

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-14318
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-30 17:15:00 UTC
Updated	2019-08-20 18:15:00 UTC
Description	Cryptopp 8.3.0 and earlier contains a timing side channel in ECDSA signature generation. This allows a local or remote attacker to recover the private key of the affected system.

Risk And Classification

Problem Types: CWE-417

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptopp	Crypto	All	All	All	All
Application	Cryptopp	Crypto	All	All	All	All

References

Reference	Source	Link
Return of the Hidden Number Problem. IACR Transactions on Cryptographic Hardware and Embedded Systems	MISC	tches.iacr.org
minerva.crocs.fi.muni.cz	MISC	minerva.crocs.fi.muni.cz
[security-announce] openSUSE-SU-2019:1968-1: moderate: Security update for libeccrypt	SUSE	lists.opensuse.org
eprint.iacr.org/2011/232.pdf	MISC	eprint.iacr.org/2011/232.pdf
Elliptic Curve timing leaks · Issue #869 · weidai11/cryptopp · GitHub	MISC	github.com
oss-security - Minerva: ECDSA key recovery from bit-length leakage	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)