CVE-2018-15560

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-15560
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-20 00:29:00 UTC
Updated	2024-01-11 15:28:00 UTC
Description	PyCryptodome before 3.6.6 has an integer overflow in the data_len variable in AESNI.c, related to the AESNI_encrypt and

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pycryptodome	Pycryptodome	All	All	All	All
Application	Python	Pycryptodome	All	All	All	All
Application	Python	Pycryptodome	All	All	All	All

References

Reference	Source	Link
Integer overflow vulnerability in pycryptodome module · Issue #198 · Legrandin/pycryptodome · GitHub	MISC	github.com
Integer overflow vulnerability in pycryptodome module	MISC	whitehatck01.blogspot.
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981045 Python (pip) Security Update for pycryptodome (GHSA-hgg3-g7gr-66r7)