CVE-2018-6594

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-6594
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-03 15:29:00 UTC
Updated	2020-07-31 19:15:00 UTC
Description	lib/Crypto/PublicKey/ElGamal.py in PyCrypto through 2.6.1 generates weak ElGamal key parameters, which allows attacke

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Dlitz	Pycrypto	All	All	All	All

References

Reference	Source	Link
Attack on PyCrypto's ElGamal Encryption with Proof-of-Concept (PoC) · Issue #253 · pycrypto/pycrypto · GitHub	MISC	github.com
[SECURITY] [DLA 1283-1] python-crypto security update	MLIST	lists.debian.o
PyCrypto: Weak key generation (GLSA 202007-62) — Gentoo security	GENTOO	security.gento

USN-3616-2: Python Crypto vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.co
USN-3616-1: Python Crypto vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.co
GitHub - TElgamal/attack-on-pycrypto-elgamal: Attack on the ElGamal Implementation of PyCrypto	MISC	github.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.

Legacy QID Mappings

670240 EulerOS Security Update for python-crypto (EulerOS-SA-2021-1836)

981278 Python (pip) Security Update for pycrypto (GHSA-6528-wvf6-f6qg)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**