



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 attackers to recover the private key.

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.org
PyCrypto: Weak key generation (GLSA 202007-62) — Gentoo security	GENTOO	security.gentoo.org

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)

© [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](#).

Free CVE JSON API cve.report/api

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