CVE-2012-2417

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

Summary

CVE	CVE-2012-2417
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-17 03:41:40 UTC
Updated	2026-04-29 01:13:23 UTC
Description	PyCrypto before 2.6 does not produce appropriate prime numbers when using an ElGamal scheme to generate a key, whic

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dlitz	Pycrypto	1.0.0	All	All	All

Application	Dlitz	Pycrypto	1.0.1	All	All	All
Application	Dlitz	Pycrypto	1.0.2	All	All	All
Application	Dlitz	Pycrypto	1.1	alpha2	All	All
Application	Dlitz	Pycrypto	1.9	alpha1	All	All
Application	Dlitz	Pycrypto	1.9	alpha2	All	All
Application	Dlitz	Pycrypto	1.9	alpha3	All	All
Application	Dlitz	Pycrypto	1.9	alpha4	All	All
Application	Dlitz	Pycrypto	1.9	alpha5	All	All
Application	Dlitz	Pycrypto	1.9	alpha6	All	All
Application	Dlitz	Pycrypto	2.0	All	All	All
Application	Dlitz	Pycrypto	2.0.1	All	All	All
Application	Dlitz	Pycrypto	2.1.0	All	All	All
Application	Dlitz	Pycrypto	2.1.0	alpha1	All	All
Application	Dlitz	Pycrypto	2.1.0	alpha2	All	All
Application	Dlitz	Pycrypto	2.1.0	beta1	All	All
Application	Dlitz	Pycrypto	2.2	All	All	All
Application	Dlitz	Pycrypto	2.3	All	All	All
Application	Dlitz	Pycrypto	2.4	All	All	All
Application	Dlitz	Pycrypto	2.4.1	All	All	All
Application	Dlitz	Pycrypto	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
oss-security - CVE-2012-2417 - PyCrypto <= 2.5 insecure ElGamal key generation	af854a3a-2127-422b-91a
[SECURITY] Fedora 15 Update: python-crypto-2.3-6.fc15	af854a3a-2127-422b-91a
[SECURITY] Fedora 16 Update: python-crypto-2.3-6.fc16	af854a3a-2127-422b-91a
www.osvdb.org/82279	af854a3a-2127-422b-91a
Malformed Request	af854a3a-2127-422b-91a
Bug #985164 “ElGamal key generation is broken” : Bugs : Python-Crypto	af854a3a-2127-422b-91a
Security Alerts - Secunia	af854a3a-2127-422b-91a
[SECURITY] Fedora 17 Update: python-crypto-2.6-1.fc17	af854a3a-2127-422b-91a
pycrypto/ChangeLog at 373ea760f21701b162e8c4912a66928ee30d401a · pycrypto/pycrypto · GitHub	af854a3a-2127-422b-91a
Support / Security / Advisories / / MDVSA-2012:117	Mandriva	af854a3a-2127-422b-91a

Support / Security / Advisories / / MDVSA-2012:117 | Mandriva	af854a3a-2127-422b-91a
IBM X-Force Exchange	af854a3a-2127-422b-91a
Debian -- Security Information -- DSA-2502-1 python-crypto	af854a3a-2127-422b-91a
Fix to bug #985164 (ElGamal key generation). Fix to missing range che… · Legrandin/pycrypto@9f912f1 · GitHub	af854a3a-2127-422b-91a
hermes.opensuse.org/messages/15083589	af854a3a-2127-422b-91a
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.