CVE-2013-1445

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

Summary

CVE	CVE-2013-1445
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-26 17:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The Crypto.Random.atfork function in PyCrypto before 2.6.1 does not properly reseed the pseudo-random number generat

Risk And Classification

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

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/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	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	2.2	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	2.5	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
Random: Make Crypto.Random.atfork() set last_reseed=None (CVE-2013-1445) · pycrypto/pycrypto@19dcf7b · GitHub	af854a3a-2127-422
oss-security - CVE-2013-1445 python-crypto: PRNG not correctly reseeded in some situations	af854a3a-2127-422
Debian -- Security Information -- DSA-2781-1 python-crypto	af854a3a-2127-422
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.