CVE-2013-7459

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

Summary

CVE	CVE-2013-7459
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-15 15:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allo

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dlitz	Pycrypto	All	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
PyCrypto: Remote execution of arbitrary code (GLSA 201702-14) — Gentoo security	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 25 Update: python-crypto-2.6.1-13.fc25 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-91ae-364da2
Throw exception when IV is used with ECB or CTR · dlitz/pycrypto@8dbe0dc · GitHub	af854a3a-2127-422b-91ae-364da2
PyCrypto 'cryptmsg.py' Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2
oss-security - Re: Buffer overflow in pycrypto	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 24 Update: python-crypto-2.6.1-13.fc24 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-91ae-364da2
cryptmsg - Writeup by Maxima [Wiki INP-net]	af854a3a-2127-422b-91ae-364da2
AES.new with invalid parameter crashes python · Issue #176 · dlitz/pycrypto · GitHub	af854a3a-2127-422b-91ae-364da2

Bug 1409754 – CVE-2013-7459 pycrypto: Heap-buffer overflow in ALGobject structure	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 24 Update: python-crypto-2.6.1-13.fc24 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 25 Update: python-crypto-2.6.1-13.fc25 - package-announce - Fedora Mailing-Lists	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710398 Gentoo Linux PyCrypto Remote execution of arbitrary code Vulnerability (GLSA 201702-14)

981123 Python (pip) Security Update for pycrypto (GHSA-cq27-v7xp-c356)