CVE-2016-9243

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

Summary

CVE	CVE-2016-9243
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-27 17:59:00 UTC
Updated	2023-11-07 02:36:00 UTC
Description	HKDF in cryptography before 1.5.2 returns an empty byte-string if used with a length less than algorithm.digest_size.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Application	Cryptography.io	Cryptography	All	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All

References

Reference	Source	Link
Python Cryptography CVE-2016-9243 Security Bypass Vulnerability	BID	www.se
[SECURITY] Fedora 24 Update: python-cryptography-1.5.3-3.fc24 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
[SECURITY] Fedora 25 Update: python-cryptography-vectors-1.5.3-1.fc25 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
Fixes #3211 -- fixed hkdf's output with short length (#3215) · pyca/cryptography@b924696 · GitHub	CONFIRM	github.c

Fixes #3211 -- fixed hkdf's output with short length (#3215) · pyca/cryptography@b924696 · GitHub	CONFIRM	github.c
[SECURITY] Fedora 23 Update: python-cryptography-vectors-1.5.3-1.fc23 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
USN-3138-1: python-cryptography vulnerability | Ubuntu	UBUNTU	www.ub
[SECURITY] Fedora 24 Update: python-cryptography-1.5.3-3.fc24 - package-announce - Fedora Mailing-Lists		lists.fed
Changelog — Cryptography 2.1.dev1 documentation	CONFIRM	cryptogr
HKDF key-length inconsistency · Issue #3211 · pyca/cryptography · GitHub	CONFIRM	github.c
oss-security - Re: CVE Request: Cryptography 1.5.3: HKDF might return an empty byte-string	MLIST	www.op
[SECURITY] Fedora 25 Update: python-cryptography-vectors-1.5.3-1.fc25 - package-announce - Fedora Mailing-Lists		lists.fed
[SECURITY] Fedora 23 Update: python-cryptography-vectors-1.5.3-1.fc23 - package-announce - Fedora Mailing-Lists		lists.fed
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

670239 EulerOS Security Update for python-cryptography (EulerOS-SA-2021-1837)

670669 EulerOS Security Update for python-cryptography (EulerOS-SA-2021-2428)