



# CVE-2016-9243

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-9243
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-27 17:59:00 UTC
<b>Updated</b>	2023-11-07 02:36:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.10	All	All	All
Application	<a href="#">Cryptography.io</a>	<a href="#">Cryptography</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	25	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	25	All	All	All

## References

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

Fixes #3211 -- fixed hkdf's output with short length (#3213) · pyca/cryptography@0924090 · 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)

© 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)