

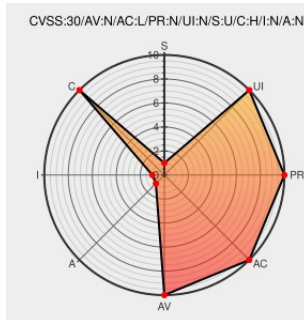


CVE-2018-10903

Published on: 07/30/2018 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:14:00 PM UTC

CVE-2018-10903

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

A flaw was found in python-cryptography versions between $\geq 1.9.0$ and < 2.3 . The `finalize_with_tag` API did not enforce a minimum tag length. If a user did not validate the input length prior to passing it to `finalize_with_tag` an attacker could craft an invalid payload with a shortened tag (e.g. 1 byte) such that they would have a 1 in 256 chance of passing the MAC check. GCM tag forgeries can cause key leakage.

CVE-2018-10903 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **[UNKNOWN]** - **python-cryptography** version **2.3**

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
-------------	------	------

 [CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10903](https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10903)

 REDHAT RHSA-2018:3600

 UBUNTU USN-3720-1

 **CONFIRM**
github.com/pyca/cryptography/pull/4342/commits/688e0f673bfbf43fa898994326c6877f00ab19ef

Related QID Numbers

981113 Python (pip) Security Update for cryptography (GHSA-fcf9-3qw3-gxmj)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Cryptography	Python-cryptography	All	All	All	All
Application	Cryptography	Python-cryptography	All	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						

cpe:2.3:a:cryptography:python-cryptography:*****:
cpe:2.3:a:cryptography:python-cryptography:*****:
cpe:2.3:a:redhat:openstack:13:*****:
cpe:2.3:a:redhat:openstack:13.0:*****:
cpe:2.3:a:redhat:openstack:13.0:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →