



# CVE-2020-13757

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

## Summary

<b>CVE</b>	CVE-2020-13757
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-01 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:16:00 UTC
<b>Description</b>	Python-RSA before 4.1 ignores leading '\0' bytes during decryption of ciphertext. This could conceivably have a security-rel

## Risk And Classification

### Problem Types: CWE-327

## 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>	14.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Python-rsa Project</a>	<a href="#">Python-rsa</a>	All	All	All	All
Application	<a href="#">Python-rsa Project</a>	<a href="#">Python-rsa</a>	4.0	All	All	All
Application	<a href="#">Python-rsa Project</a>	<a href="#">Python-rsa</a>	4.0	All	All	All

## References

Reference	Source
[SECURITY] Fedora 32 Update: python-rsa-3.4.2-15.fc32 - package-announce - Fedora Mailing-Lists	FE
[SECURITY] Fedora 31 Update: python-rsa-3.4.2-15.fc31 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 32 Update: python-rsa-3.4.2-15.fc32 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 31 Update: python-rsa-3.4.2-15.fc31 - package-announce - Fedora Mailing-Lists	FE
USN-4478-1: Python-RSA vulnerability   Ubuntu security notices   Ubuntu	UI
python-rsa does not detect ciphertext modification (prepended "0" bytes) in PKCS1_v1_5 · Issue #146 · sybrenstuvell/python-rsa · GitHub	Co
python-rsa does not detect ciphertext modification (prepended "0" bytes) in PKCS1_v1_5 · Issue #146 · sybrenstuvell/python-rsa · GitHub	M
CVE Program record	C'

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[750659](#) SUSE Enterprise Linux Security Update for python-rsa (SUSE-SU-2021:2008-1)

[750702](#) OpenSUSE Security Update for python-rsa (openSUSE-SU-2021:0901-1)

[750780](#) OpenSUSE Security Update for python-rsa (openSUSE-SU-2021:2008-1)

[982888](#) Python (pip) Security Update for rsa (GHSA-537h-rv9q-vvph)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)