CVE-2020-13757

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13757
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-01 19:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	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	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Python-rsa Project	Python-rsa	All	All	All	All
Application	Python-rsa Project	Python-rsa	4.0	All	All	All
Application	Python-rsa Project	Python-rsa	4.0	All	All	All

References

Reference	So
[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 · sybrenstuvel/python-rsa · GitHub	CO
python-rsa does not detect ciphertext modification (prepended "0" bytes) in PKCS1_v1_5 · Issue #146 · sybrenstuvel/python-rsa · GitHub	M
CVE Program record	CV

NVD vulnerability detail N

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)