CVE-2020-25658

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25658
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-12 14:15:00 UTC
Updated	2023-02-12 23:40:00 UTC
Description	It was found that python-rsa is vulnerable to Bleichenbacher timing attacks. An attacker can use this flaw via the RSA decry

Risk And Classification

Problem Types: CWE-385

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Python-rsa Project	Python-rsa	All	All	All	All
Application	Python-rsa Project	Python-rsa	All	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Openstack Platform	16.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Openstack Platform	16.0	All	All	All

References

Reference	Sou
[SECURITY] Fedora 35 Update: python-rsa-4.7.2-1.fc35 - package-announce - Fedora Mailing-Lists	MIS
1889972 – (CVE-2020-25658) CVE-2020-25658 python-rsa: bleichenbacher timing oracle attack against RSA decryption	MIS
[SECURITY] Fedora 35 Update: python-rsa-4.7.2-1.fc35 - package-announce - Fedora Mailing-Lists	FED
Red Hat Customer Portal - Access to 24x7 support and knowledge	MIS
Red Hat Customer Portal - Access to 24x7 support and knowledge	MIS

[SECURITY] Fedora 33 Update: python-rsa-4.7.2-1.fc33 - package-announce - Fedora Mailing-Lists	MIS
[SECURITY] Fedora 33 Update: python-rsa-4.7.2-1.fc33 - package-announce - Fedora Mailing-Lists	FED
1889972 – (CVE-2020-25658) CVE-2020-25658 python-rsa: bleichenbacher timing oracle attack against RSA decryption	CON
[SECURITY] Fedora 34 Update: python-rsa-4.7.2-1.fc34 - package-announce - Fedora Mailing-Lists	FED
Red Hat Customer Portal - Access to 24x7 support and knowledge	MIS
CVE-2020-25658 - Bleichenbacher-style timing oracle in PKCS#1 v1.5 decryption code · Issue #165 · sybrenstuvel/python-rsa · GitHub	MIS
Red Hat Customer Portal - Access to 24x7 support and knowledge	MIS
[SECURITY] Fedora 34 Update: python-rsa-4.7.2-1.fc34 - package-announce - Fedora Mailing-Lists	MIS
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 240265 Red Hat Update for red hat ceph storage 4.3 (RHSA-2022:1716)
- 281931 Fedora Security Update for python (FEDORA-2021-c1fef03e71)
- 281932 Fedora Security Update for python (FEDORA-2021-783a157adc)
- 355597 Amazon Linux Security Advisory for python-rsa : ALAS2-2023-2150
- 752780 SUSE Enterprise Linux Security Update for python-rsa (SUSE-SU-2022:3932-1)
- 770064 Red Hat OpenShift Container Platform 4.7.0 Packages and Security Update (RHSA-2020:5634)
- 900224 CBL-Mariner Linux Security Update for python-rsa 4.7.2
- 980658 Python (pip) Security Update for rsa (GHSA-xrx6-fmxq-rjj2)