CVE-2019-14859

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-14859
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-02 15:15:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	A flaw was found in all python-ecdsa versions before 0.13.3, where it did not correctly verify whether signatures used DER

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python-ecdsa Project	Python-ecdsa	All	All	All	All
Application	Python-ecdsa Project	Python-ecdsa	All	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	3.0	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	3.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	15	All	All	All
Application	Redhat	Openstack	15.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	15.0	All	All	All

Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
Release ecdsa 0.13.3 · warner/python-ecdsa · GitHub	MISC	github.com
1760843 – (CVE-2019-14859) CVE-2019-14859 python-ecdsa: DER encoding is not being verified in signatures	CONFIRM	bugzilla.redha
ecdsa · PyPI	MISC	pypi.org
Inconsistent handling of malformed DER signatures · Issue #114 · warner/python-ecdsa · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

239895 Red Hat Update for Satellite 6.10 (RHSA-2021:4702)

355760 Amazon Linux Security Advisory for python-ecdsa : ALAS-2023-1800

501363 Alpine Linux Security Update for py3-ecdsa

505306 Alpine Linux Security Update for py3-ecdsa

670670 EulerOS Security Update for python-ecdsa (EulerOS-SA-2021-2429)

690472 Free Berkeley Software Distribution (FreeBSD) Security Update for security/py-ecdsa (a23ebf36-e8b6-4665-b0f3-4c977f9a145c)

981345 Python (pip) Security Update for ecdsa (GHSA-8qxj-f9rh-9fg2)