



CVE-2019-14853

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

Summary

CVE	CVE-2019-14853
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-26 13:15:00 UTC
Updated	2019-12-17 23:15:00 UTC
Description	An error-handling flaw was found in python-ecdsa before version 0.13.3. During signature decoding, malformed DER signal

Risk And Classification

Problem Types: CWE-755

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

References

Reference	Source
Release ecdsa 0.13.3 · warner/python-ecdsa · GitHub	MISC
Debian -- Security Information -- DSA-4588-1 python-ecdsa	DEB
1758704 – (CVE-2019-14853) CVE-2019-14853 python-ecdsa: Unexpected and undocumented exceptions during signature decoding	CONF
Bugtraq: [SECURITY] [DSA 4588-1] python-ecdsa security update	BUG
CVE Program record	CVE
NVD vulnerability detail	NVD

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
690472 Free Berkeley Software Distribution (FreeBSD) Security Update for security/py-ecdsa (a23ebf36-e8b6-4665-b0f3-4c977f9a145c)
981445 Python (pip) Security Update for ecdsa (GHSA-pwfw-mgfj-7g3g)
983465 Python (pip) Security Update for ecdsa (GHSA-2mrj-435v-c2cr)

© [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](#)