CVE-2017-2592

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-2592
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-08 17:29:00 UTC
Updated	2019-10-09 23:26:00 UTC
Description	python-oslo-middleware before versions 3.8.1, 3.19.1, 3.23.1 is vulnerable to an information disclosure. Software using the

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Application	Openstack	Oslo.middleware	All	All	All	All
Application	Openstack	Oslo.middleware	All	All	All	All
Application	Openstack	Oslo.middleware	All	All	All	All

References

Reference
Gerrit Code Review
1414698 – (CVE-2017-2592) CVE-2017-2592 python-oslo-middleware: CatchErrors leaks sensitive values into error logs
OpenStack oslo.middleware CVE-2017-2592 Information Disclosure Vulnerability
Gerrit Code Review
Red Hat Customer Portal
Red Hat Customer Portal
USN-3666-1: Oslo middleware vulnerability | Ubuntu security notices | Ubuntu
Red Hat Customer Portal
OpenStack Open Source Cloud Computing Software » Message: [openstack-announce] [OSSA-2017-001] CatchErrors leaks sensitive values

Red Hat Customer Portal
Bug #1628031 “[OSSA-2017-001] CatchErrors leaks sensitive values...” : Bugs : keystonemiddleware
Gerrit Code Review
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980794 Python (pip) Security Update for oslo.middleware (GHSA-xcp8-hh74-f6mc)