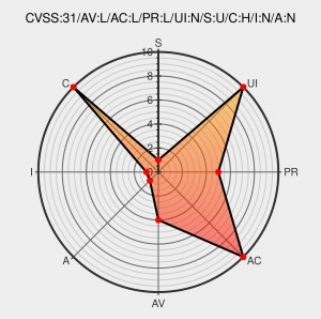
# CVE-2012-5476

Published on: 12/30/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:13 AM UTC

## CVE-2012-5476

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Debian Linux from Debian contain the following vulnerability:

Within the RHOS Essex Preview (2012.2) of the OpenStack dashboard package, the file /etc/quantum/quantum.conf is world readable which exposes the admin password and token value.

CVE-2012-5476 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **openstack-dashboard** - **openstack-dashboard** version **= RHOS Essex Preview (2012.2)**

### CVSS3 Score: 5.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | NONE | NONE |

### CVSS2 Score: 2.1 - LOW

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| CVE-2012-5476 | Third Party Advisory<br>security-tracker.debian.org<br>text/html | MISC security-tracker.debian.org/tracker/CVE-2012-5476 |

| | | |
|---|---|---|
| 873524 – (CVE-2012-5476) CVE-2012-5476 OpenStack: Quantum /etc/quantum/quantum.conf secret password and token exposure | Issue Tracking<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | MISC<br>bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-5476 |
| CVE-2012-5476 - Red Hat Customer Portal | Third Party Advisory<br>access.redhat.com<br>text/html | MISC<br>access.redhat.com/security/cve/cve-2012-5476 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Openstack | Horizon | 2012.2 | All | All | All |
| Application | Openstack | Horizon | 2012.2 | All | All | All |

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:horizon:2012.2:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:horizon:2012.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→



**CVE.report and Source URL Uptime Status status.cve.report**