



# CVE-2015-6927

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-6927                                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2015-09-28 20:59:00 UTC                                                                                                      |
| <b>Updated</b>         | 2017-07-01 01:29:00 UTC                                                                                                      |
| <b>Description</b>     | vzctl before 4.9.4 determines the virtual environment (VE) layout based on the presence of root.hdd/DiskDescriptor.xml in tl |

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product               | Version | Update | Edition | Language |
|-------------|------------------------|-----------------------|---------|--------|---------|----------|
| Application | <a href="#">Openvz</a> | <a href="#">Vzctl</a> | All     | All    | All     | All      |

## References

| Reference                                                 | Source  | Link                                | Tags                |
|-----------------------------------------------------------|---------|-------------------------------------|---------------------|
| Download/vzctl/4.9.4 - OpenVZ Virtuozzo Containers Wiki   | CONFIRM | <a href="#">openvz.org</a>          | Patch               |
| vzctl: Security bypass (GLSA 201701-30) — Gentoo security | GENTOO  | <a href="#">security.gentoo.org</a> |                     |
| OpenVZ-legacy / vzctl / 9e98ea630ac - Stash               | CONFIRM | <a href="#">src.openvz.org</a>      | Exploit             |
| Debian -- Security Information -- DSA-3357-1 vzctl        | DEBIAN  | <a href="#">www.debian.org</a>      |                     |
| CVE Program record                                        | CVE.ORG | <a href="#">www.cve.org</a>         | canonical           |
| NVD vulnerability detail                                  | NVD     | <a href="#">nvd.nist.gov</a>        | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710515](#) Gentoo Linux vzctl Security bypass Vulnerability (GLSA 201701-30)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)