# CVE-2009-3525

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2009-3525 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2009-10-05 19:30:00 UTC |
| **Updated** | 2017-09-19 01:29:00 UTC |
| **Description** | The pyGrub boot loader in Xen 3.0.3, 3.3.0, and Xen-3.3.1 does not support the password option in grub.conf for para-virtu |

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Xen | Xen | 3.0.3 | All | All | All |
| Application | Xen | Xen | 3.3.0 | All | All | All |
| Application | Xen | Xen | 3.3.1 | All | All | All |
| Application | Xen | Xen | 3.0.3 | All | All | All |
| Application | Xen | Xen | 3.3.0 | All | All | All |
| Application | Xen | Xen | 3.3.1 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Bug 525740 – CVE-2009-3525 Xen: PyGrub missing support for password configuration command | CONFIRM | bugzilla.re |
| Support | REDHAT | www.redha |
| Bug 525740 – CVE-2009-3525 Xen: PyGrub missing support for password configuration command | CONFIRM | bugzilla.re |
| SecurityTracker.com Archives - Xen PyGrub Access Control Flaw Lets Local Users Modify the Boot Configuration | SECTRACK | www.secu |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2010:012 | SUSE | lists.opens |
| xen-unstable.hg: log | CONFIRM | xenbits.xe |
| Xen pygrub Local Authentication Bypass Vulnerability | BID | www.secu |
| Repository / Oval Repository | OVAL | oval.cisecu |

| | | |
|---|---|---|
| Security Advisory SA36908 - Red Hat update for xen - Secunia | SECUNIA | secunia.co |
| oss-security - CVE Request -- Xen -- PyGrub | MLIST | www.open |
| CVE Program record | CVE.ORG | www.cve.c |
| NVD vulnerability detail | NVD | nvd.nist.gc |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.