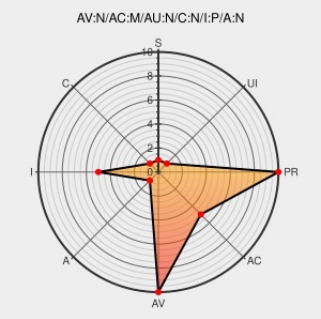
# CVE-2013-4314

Published on: 09/30/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

## CVE-2013-4314

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




Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The X509Extension in pyOpenSSL before 0.13.1 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.

CVE-2013-4314 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| oss-security - Re: CVE request: pyOpenSSL hostname check bypassing vulnerability | www.openwall.com text/html | MLIST [oss-security] 20130906 Re: CVE request: pyOpenSSL hostname check bypassing vulnerability |
| Debian -- Security Information -- DSA-2763-1 pyopenssl | www.debian.org Depreciated Link text/html | DEBIAN DSA-2763 |
| Bug 1005325 – CVE-2013-4314 pyOpenSSL: hostname check bypassing vulnerability | bugzilla.redhat.com text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1005325 |
| USN-1965-1: pyOpenSSL vulnerability \| Ubuntu | Vendor Advisory www.ubuntu.com text/html | UBUNTU USN-1965-1 |
| [pyOpenSSL-Users] pyOpenSSL 0.13.1 | mail.python.org | MLIST [pyOpenSSL-Users] 20130904 pyOpenSSL 0.13.1 |

| | | |
|---|---|---|
| | text/html | |
| openSUSE-SU-2013:1648-1: moderate: update for python-pyOpenSSL | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2013:1648 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 10.04 | - | lts | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | - | lts | All |
| Operating System | Canonical | Ubuntu Linux | 12.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 13.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 10.04 | - | lts | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | - | lts | All |
| Operating System | Canonical | Ubuntu Linux | 12.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 13.04 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.10 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | a1 | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | a2 | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.12 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.7 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.8 | a1 | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.9 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | All | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.10 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | a1 | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.11 | a2 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Jean-paul Calderone | Pyopenssl | 0.12 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.7 | All | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.8 | a1 | All | All |
| Application | Jean-paul Calderone | Pyopenssl | 0.9 | All | All | All |

cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.10:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:a1:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:a2:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.12:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.8:a1:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.9:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:*:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.10:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:a1:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.11:a2:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.12:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.8:a1:*:*:*:*:*:*:

cpe:2.3:a:jean-paul_calderone:pyopenssl:0.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→



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