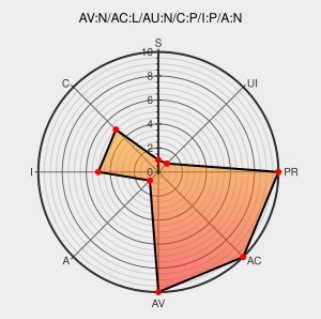
CVE-2014-3694

Published on: 10/29/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-3694

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



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

The (1) bundled GnuTLS SSL/TLS plugin and the (2) bundled OpenSSL SSL/TLS plugin in libpurple in Pidgin before 2.10.10 do not properly consider the Basic Constraints extension during verification of X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

CVE-2014-3694 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
openSUSE-SU-2014:1376-1: moderate: update for pidgin	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2014:1376
openSUSE-SU-2014:1397-1: moderate: update for pidgin	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2014:1397
Security Advisory SA61968 - Ubuntu update for pidgin - Secunia	web.archive.org, text/html	SECUNIA 61968
pidgin/main: changeset 2e4475087f04	Issue Tracking, hg.pidgin.im, text/xml	CONFIRM hg.pidgin.im/pidgin/main/rev/2e4475087f04

USN-2390-1: Pidgin vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2390-1
Pidgin Security Advisories	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM pidgin.im/news/security/?id=86
Debian -- Security Information -- DSA-3055-1 pidgin	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3055
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2017:1854
Security Advisory SA60741 - Debian update for pidgin - Secunia	web.archive.org text/html	SECUNIA 60741

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating	Opensuse	Opensuse	13.2	All	All	All

System						
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	All	All	All
Application	Pidgin	Pidgin	2.10.7	All	All	All
Application	Pidgin	Pidgin	2.10.8	All	All	All
Application	Pidgin	Pidgin	2.10.0	All	All	All
Application	Pidgin	Pidgin	2.10.1	All	All	All
Application	Pidgin	Pidgin	2.10.2	All	All	All
Application	Pidgin	Pidgin	2.10.3	All	All	All
Application	Pidgin	Pidgin	2.10.4	All	All	All
Application	Pidgin	Pidgin	2.10.5	All	All	All
Application	Pidgin	Pidgin	2.10.6	All	All	All
Application	Pidgin	Pidgin	2.10.7	All	All	All
Application	Pidgin	Pidgin	2.10.8	All	All	All
Application	Pidgin	Pidgin	All	All	All	All

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.0:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.1:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.2:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.3:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.4:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.5:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.6:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.7:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.8:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.0:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.1:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.2:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.3:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.4:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.5:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.6:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.7:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:2.10.8:*:*:*:*:*:*:*

cpe:2.3:a:pidgin:pidgin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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