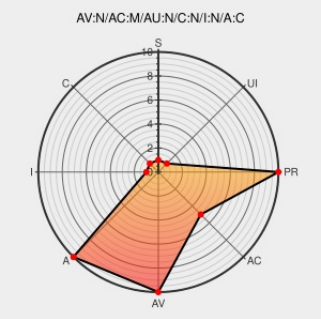
CVE-2015-2696

Published on: 11/08/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-2696

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



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

lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a gss_inquire_context call.

CVE-2015-2696 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
RT/krbdev.mit.edu: Ticket #8244 SPNEGO and IAKERB context aliasing bugs [CVE-2015-2695] [CVE-2015-2696]	Vendor Advisory, krbdev.mit.edu, text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=8244
Fix IAKERB context aliasing bugs [CVE-2015-2696] · krb5/krb5@e04f028 · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/krb5/krb5/commit/e04f0283516e80d2f93366e0d479d13c9b5c8c2a
[security-announce] SUSE-SU-2015:1897-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SU-2015:1897

[security-announce] openSUSE-SU-2015:1997-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1997
Debian -- Security Information -- DSA-3395-1 krb5	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3395
MIT Kerberos 5 CVE-2015-2696 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 90675
MIT Kerberos 5: Multiple vulnerabilities (GLSA 201611-14) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201611-14
MIT Kerberos Multiple Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034084
[security-announce] openSUSE-SU-2015:1928-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1928
USN-2810-1: Kerberos vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2810-1

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	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	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	15.04	All	All	All

Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All

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

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

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

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

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:7.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:mit:kerberos_5:*:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

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

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

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

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

cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_software_development_kit:12:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_software_development_kit:12:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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