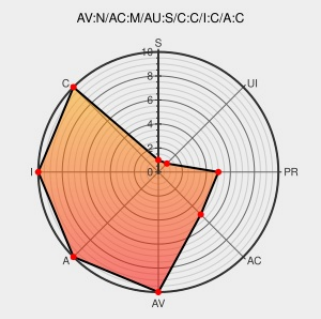
CVE-2015-2698

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

Last Modified on: 03/23/2021 11:26:20 PM UTC

CVE-2015-2698

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



Certain versions of Kerberos 5 from Mit contain the following vulnerability:

The iakerb_gss_export_sec_context function in lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) 1.14 pre-release 2015-09-14 improperly accesses a certain pointer, which allows remote authenticated users to cause a denial of service (memory corruption) or possibly have unspecified other impact by interacting with an application that calls the gss_export_sec_context function. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-2696.

CVE-2015-2698 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
RT/krbdev.mit.edu: Ticket #8273 Fix IAKERB context export/import [CVE-2015-2698]	Vendor Advisory, krbdev.mit.edu, text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=8273
Fix IAKERB context export/import [CVE-2015-2698] · krb5/krb5@3db8dfe · GitHub	github.com, text/html	CONFIRM github.com/krb5/krb5/commit/3db8dfec1ef50ddd78d6ba9503185995876a39fd
openSUSE-SU-2015:2055-1: moderate: Security update for krb5	lists.opensuse.org, text/html	SUSE openSUSE-SU-2015:2055
openSUSE-SU-2015:2376-1:	lists.opensuse.org	SUSE openSUSE-SU-2015:2376

moderate: Security update for krb5	text/html	
USN-2810-1: Kerberos vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2810-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	1.14	beta2	All	All
Application	Mit	Kerberos 5	1.14	beta2	All	All

cpe:2.3:a:mit:kerberos_5:1.14:beta2:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.14:beta2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→