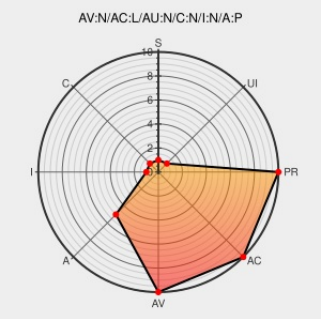
CVE-2013-1415

Published on: 03/02/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:32 PM UTC

CVE-2013-1415

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



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

The pkinit_check_kdc_pkid function in plugins/preauth/pkinit/pkinit_crypto_openssl.c in the PKINIT implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.4 and 1.11.x before 1.11.1 does not properly handle errors during extraction of fields from an X.509 certificate, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a malformed KRB5_PADATA_PK_AS_REQ AS-REQ request.

CVE-2013-1415 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Support / Security / Advisories / / MDVSA-2013:157 | Mandriva	Third Party Advisory, www.mandriva.com, text/html	MANDRIVA MDVSA-2013:157
RT/krbdev.mit.edu: Ticket #7570 PKINIT null pointer deref [CVE-2013-1415]	Vendor Advisory, krbdev.mit.edu, text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=7570
PKINIT null pointer deref [CVE-2013-1415] · krb5/krb5@f249555 · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/krb5/krb5/commit/f249555301940c6df3a2cdda13b56b5674eebc2e

openSUSE-SU-2013:0523-1: moderate: krb5: security fix for PKINIT plugin	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0523
RT/krbdev.mit.edu: Ticket #7577 PKINIT null pointer deref [CVE-2013-1415]	Vendor Advisory krbdev.mit.edu text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=7577
Kerberos 5 Release 1.11.4	Release Notes Vendor Advisory web.mit.edu text/html	CONFIRM web.mit.edu/kerberos/www/krb5-1.11/
Security Advisory SA55040 - Oracle Solaris Key Distribution Center (KDC) Denial of Service Vulnerabilities - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 55040
Kerberos 5 Release 1.10.6	Release Notes Vendor Advisory web.mit.edu text/html	CONFIRM web.mit.edu/kerberos/www/krb5-1.10/

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	All	All	All	All
Application	Mit	Kerberos 5	1.11	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Application	Mit	Kerberos 5	1.11	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All

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

cpe:2.3:a:mit:kerberos_5:1.11:*:*:*:*:*:*:*:

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

cpe:2.3:a:mit:kerberos_5:1.11:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→