CVE-2009-4212

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-4212
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-01-13 19:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple integer underflows in the (1) AES and (2) RC4 decryption functionality in the crypto library in MIT Kerberos 5 (aka k

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos	5-1.6.3	All	All	All

Application	Mit	Kerberos 5	1.3	All	All	All
Application	Mit	Kerberos 5	1.3.1	All	All	All
Application	Mit	Kerberos 5	1.3.2	All	All	All
Application	Mit	Kerberos 5	1.3.3	All	All	All
Application	Mit	Kerberos 5	1.3.4	All	All	All
Application	Mit	Kerberos 5	1.3.5	All	All	All
Application	Mit	Kerberos 5	1.3.6	All	All	All
Application	Mit	Kerberos 5	1.4	All	All	All
Application	Mit	Kerberos 5	1.4.1	All	All	All
Application	Mit	Kerberos 5	1.4.2	All	All	All
Application	Mit	Kerberos 5	1.4.3	All	All	All
Application	Mit	Kerberos 5	1.4.4	All	All	All
Application	Mit	Kerberos 5	1.5	All	All	All
Application	Mit	Kerberos 5	1.5.1	All	All	All
Application	Mit	Kerberos 5	1.5.2	All	All	All
Application	Mit	Kerberos 5	1.5.3	All	All	All
Application	Mit	Kerberos 5	1.6	All	All	All
Application	Mit	Kerberos 5	1.6.1	All	All	All
Application	Mit	Kerberos 5	1.6.2	All	All	All
Application	Mit	Kerberos 5	1.7	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sc
MIT Kerberos AES and RC4 Decryption Integer Underflow Vulnerabilities	af
Security Advisory SA38203 - Fedora update for krb5 - Secunia	af
Security Advisory SA38140 - Debian update for krb5 - Secunia	af
USN-881-1: Kerberos vulnerability | Ubuntu	af
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Community	af
Debian -- Security Information -- DSA-1969-1 krb5	af
Avaya Products Multiple Vulnerabilities - Advisories - Community	af
Sun Solaris Kerberos Integer Underflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af
web.mit.edu/kerberos/advisories/MITKRB5-SA-2009-004.txt	af
Security Advisory SA38108 - Red Hat update for krb5 - Secunia	af

Security Advisory SA38108 - Red Hat update for krb5 - Secunia	af
[SECURITY] Fedora 11 Update: krb5-1.6.3-23.fc11	af
Repository / Oval Repository	af
sunsolve.sun.com/search/document.do	af
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af
[SECURITY] Fedora 12 Update: krb5-1.7-18.fc12	af
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af
rhn.redhat.com | Red Hat Support	af
Repository / Oval Repository	af
Repository / Oval Repository	af
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af
sunsolve.sun.com/search/document.do	af
Bug 545015 – CVE-2009-4212 krb: KDC integer overflows in AES and RC4 decryption routines (MITKRB5-SA-2009-004)	af
Red Hat Customer Portal	af
Support / Security / Advisories / / MDVSA-2010:006 | Mandriva	af
About the security content of Security Update 2010-004 / Mac OS X v10.6.4	af
'[security bulletin] HPSBOV02682 SSRT100495 rev.1 - HP OpenVMS running Kerberos, Remote Denial of Ser' - MARC	af
ASA-2010-053 (RHSA-2010-0039)	af
Ubuntu update for krb5 - Secunia Advisories - Vulnerability Information - Secunia.com	af
APPLE-SA-2010-06-15-1 Security Update 2010-004 / Mac OS X v10.6.4	af
Kerberos AES and RC4 Integer Underflow May Let Remote Users Execute Arbitrary Code - SecurityTracker	af
Kerberos KDC RC4 and AES Decryption Integer Underflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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