CVE-2011-0285

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

Summary

CVE	CVE-2011-0285
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-15 00:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The process_chpw_request function in schpw.c in the password-changing functionality in kadmind 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-20 | 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	1.7	All	All	All

Application	Mit	Kerberos 5	1.7.1	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
Application	Mit	Kerberos 5	1.9	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
RT/krbdev.mit.edu: Ticket #6899 kadmind frees invalid pointer [MITKRB5-SA-2011-004 CVE-2011-0285]	af854a3a-2127-422b-91ae-364da2
web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-004.txt	af854a3a-2127-422b-91ae-364da2
[SECURITY] Fedora 15 Update: krb5-1.9-7.fc15	af854a3a-2127-422b-91ae-364da2
Red Hat update for krb5 - Secunia.com	af854a3a-2127-422b-91ae-364da2
Kerberos kadmind Can Be Crashed By a Remote Users Conducting an NMAP Scan - SecurityTracker	af854a3a-2127-422b-91ae-364da2
Support / Security / Advisories / / MDVSA-2011:077 | Mandriva	af854a3a-2127-422b-91ae-364da2
MIT Kerberos kadmind Change Password Feature Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
Support	af854a3a-2127-422b-91ae-364da2
SUSE update for krb5 - Secunia.com	af854a3a-2127-422b-91ae-364da2
hermes.opensuse.org/messages/8086843	af854a3a-2127-422b-91ae-364da2
osvdb.org/71789	af854a3a-2127-422b-91ae-364da2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
#621726 - krb5-admin-server: kadmind dies after nmap -sV - Debian Bug report logs	af854a3a-2127-422b-91ae-364da2
Kerberos kadmind Denial of Service Vulnerability - Secunia.com	af854a3a-2127-422b-91ae-364da2
SecurityFocus	af854a3a-2127-422b-91ae-364da2
CXSecurity - IDS	af854a3a-2127-422b-91ae-364da2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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