CVE-2000-0392

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

Summary

CVE	CVE-2000-0392
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-05-16 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in ksu in Kerberos 5 allows local users to gain root privileges.

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/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	Cygnus	Cygnus Network Security	4.0	All	All	All
Application	Cygnus	Kerbnet	5.0	All	All	All

Application	Mit	Kerberos	4.0	All	All	All
Application	Mit	Kerberos 5	1.0	All	All	All
Application	Mit	Kerberos 5	1.1.1	All	All	All
Operating System	Redhat	Linux	6.2	All	alpha	All
Operating System	Redhat	Linux	6.2	All	i386	All
Operating System	Redhat	Linux	6.2	All	sparc	All

Vendor Declared Affected Products

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

References

Reference	Source
Multiple Vendor Kerberos 5/Kerberos 4 Compatibility krb_rd_req() Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108
archives.neohapsis.com/archives/freebsd/2000-05/0295.html	af854a3a-2127-422b-91ae-364da2661108
redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108
archives.neohapsis.com/archives/bugtraq/2000-05/0184.html	af854a3a-2127-422b-91ae-364da2661108
CERT Advisory CA-2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services	af854a3a-2127-422b-91ae-364da2661108
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.