CVE-2008-3825

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

Summary

CVE	CVE-2008-3825
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-03 15:07:00 UTC
Updated	2018-10-11 20:49:00 UTC
Description	pam_krb5 2.2.14 in Red Hat Enterprise Linux (RHEL) 5 and earlier, when the existing_ticket option is enabled, uses incorre

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	5	unknown	server	All
Operating System	Redhat	Enterprise Linux	5	unknown	server	All
Operating System	Redhat	Enterprise Linux Desktop	5	unknown	client	All
Operating System	Redhat	Enterprise Linux Desktop	5	unknown	client	All

References

Reference	Source
SecurityTracker.com Archives - pam_krb5 Credential Cache Permissions Bug Let Local Users Gain Elevated Privileges	SECTRACK
pam_krb5 Credential Cache "exisiting_ticket" Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
[SECURITY] Fedora 9 Update: pam_krb5-2.3.0-2.fc9	FEDORA
Fedora update for pam_krb5 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
SecurityFocus	BUGTRAQ
VMSA-2011-0003	CONFIRM
pam_krb5 Existing Ticket Configuration Option Local Privilege Escalation Vulnerability	BID
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:027	SUSE
Bug 461960 – CVE-2008-3825 pam_krb5 existing_ticket permission flaw	CONFIRM
Repository / Oval Repository	OVAL

IBM X-Force Exchange	XF
Advisories | Mandriva	MANDRIVA
[SECURITY] Fedora 8 Update: pam_krb5-2.2.18-2.fc8	FEDORA
VMware ESX Server pam_krb5 Security Issues - Secunia.com	SECUNIA
Red Hat update for pam_krb5 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
rhn.redhat.com | Red Hat Support	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2017-09-28	Joshua Bressers	This issue did not affect the version of pam_krb5 shipped in Red Hat Enterprise Linux 2.1, 3

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