



CVE-2011-1758

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

Summary

CVE	CVE-2011-1758
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-26 18:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The krb5_save_ccname_done function in providers/krb5/krb5_auth.c in System Security Services Daemon (SSSD) 1.5.x before 1.5.10 does not properly validate the length of the data being saved, which allows local users to cause a denial of service via a crafted krb5_auth.c file.

Risk And Classification

Primary CVSS: v2.0 3.7 from nvd@nist.gov

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

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Sssd	1.5.0	All	All	All

Application	Fedoraproject	Sssd	1.5.1	All	All	All
Application	Fedoraproject	Sssd	1.5.2	All	All	All
Application	Fedoraproject	Sssd	1.5.3	All	All	All
Application	Fedoraproject	Sssd	1.5.4	All	All	All
Application	Fedoraproject	Sssd	1.5.5	All	All	All
Application	Fedoraproject	Sssd	1.5.6	All	All	All
Application	Fedoraproject	Sssd	1.5.6.1	All	All	All

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

References	
Reference	Source
Fedora Hosted Git Repositories - sssd.git/commit	af854a3a-7c00-4000-9000-000000000000
Bug 700867 – CVE-2011-1758 sssd: automatic TGT renewal overwrites cached password with value of predicatable filename	af854a3a-7c00-4000-9000-000000000000
oss-security - vulnerability in sssd 1.5.0+ (CVE-2011-1758)	af854a3a-7c00-4000-9000-000000000000
Infrastructure/Fedorahosted-retirement - Fedora Project Wiki	af854a3a-7c00-4000-9000-000000000000
Bug 700891 – CVE-2011-1758 sssd: automatic TGT renewal overwrites cached password with predicatable filename [fedora-all]	af854a3a-7c00-4000-9000-000000000000
Issue #856: Automatic TGT renewal overwrites cached password - sssd - Pagure.io	af854a3a-7c00-4000-9000-000000000000
[SECURITY] Fedora 14 Update: sssd-1.5.7-1.fc14	af854a3a-7c00-4000-9000-000000000000
Releases/Notes-1.5.7 – SSSD	af854a3a-7c00-4000-9000-000000000000
[SECURITY] Fedora 15 Update: sssd-1.5.7-1.fc15	af854a3a-7c00-4000-9000-000000000000
Fedora Hosted Git Repositories - sssd.git/commit	MITRE
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