# CVE-2014-5351

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-5351 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-10-10 01:55:00 UTC |
| **Updated** | 2020-01-21 15:46:00 UTC |
| **Description** | The kadm5_randkey_principal_3 function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) before 1. |

## Risk And Classification

**Problem Types:** CWE-255

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Mit | Kerberos 5 | 1.12.2 | All | All | All |
| Application | Mit | Kerberos 5 | 1.12.2 | All | All | All |

## References

| Reference |
|---|
| USN-2498-1: Kerberos vulnerabilities \| Ubuntu |
| openSUSE-SU-2015:0255-1: moderate: Security update for krb5 |
| Kerberos kadmin randkey Function Lets Remote Authenticated Administrators Obtain Old Keys and Potentially Forge Tickets - SecurityTracke |
| [SECURITY] [DLA 1265-1] krb5 security update |
| Support / Security / Advisories / / MDVSA-2014:224 \| Mandriva |
| [SECURITY] Fedora 20 Update: krb5-1.11.5-18.fc20 |
| #8018: Return only new keys in randkey [CVE-2014-5351] |
| IBM X-Force Exchange |
| Return only new keys in randkey [CVE-2014-5351] · krb5/krb5@af0ed4d · GitHub |
| Mageia Advisory: MGASA-2014-0477 - Updated krb5 packages fix security vulnerability |
| MIT Kerberos 5 'svr_principal.c' Information Disclosure Vulnerability |
| Bug 1145425 – CVE-2014-5351 krb5: current keys returned when randomizing the keys for a service principal |

| |
|---|
| [SECURITY] Fedora 21 Update: krb5-1.12.2-9.fc21 |
| [security-announce] SUSE-SU-2015:0290-1: important: Security update for |
| MIT Kerberos 5: User-assisted execution of arbitrary code (GLSA 201412-53) — Gentoo security |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

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