CVE-2014-4343

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

Summary

CVE	CVE-2014-4343
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-14 05:01:00 UTC
Updated	2020-01-21 15:46:00 UTC
Description	Double free vulnerability in the init_ctx_reselect function in the SPNEGO initiator in lib/gssapi/spnego/spnego_mech.c in MI

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mit	Kerberos 5	1.10	All	All	All
Application	Mit	Kerberos 5	1.10.1	All	All	All
Application	Mit	Kerberos 5	1.10.2	All	All	All
Application	Mit	Kerberos 5	1.10.3	All	All	All
Application	Mit	Kerberos 5	1.10.4	All	All	All
Application	Mit	Kerberos 5	1.11	All	All	All
Application	Mit	Kerberos 5	1.11.1	All	All	All
Application	Mit	Kerberos 5	1.11.2	All	All	All
Application	Mit	Kerberos 5	1.11.3	All	All	All
Application	Mit	Kerberos 5	1.11.4	All	All	All
Application	Mit	Kerberos 5	1.11.5	All	All	All
Application	Mit	Kerberos 5	1.12	All	All	All
Application	Mit	Kerberos 5	1.12.1	All	All	All
Application	Mit	Kerberos 5	1.10	All	All	All
Application	Mit	Kerberos 5	1.10.1	All	All	All

Application	Mit	Kerberos 5	1.10.2	All	All	All
Application	Mit	Kerberos 5	1.10.3	All	All	All
Application	Mit	Kerberos 5	1.10.4	All	All	All
Application	Mit	Kerberos 5	1.11	All	All	All
Application	Mit	Kerberos 5	1.11.1	All	All	All
Application	Mit	Kerberos 5	1.11.2	All	All	All
Application	Mit	Kerberos 5	1.11.3	All	All	All
Application	Mit	Kerberos 5	1.11.4	All	All	All
Application	Mit	Kerberos 5	1.11.5	All	All	All
Application	Mit	Kerberos 5	1.12	All	All	All
Application	Mit	Kerberos 5	1.12.1	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	L
Security Advisory SA61052 - F5 Multiple Products Kerberos GSSAPI SPNEGO Memory Corruption Vulnerability - Secunia	SECUNIA	s
Red Hat Customer Portal	REDHAT	rh
MIT Kerberos 5 CVE-2014-4343 Remote Denial of Service Vulnerability	BID	w
Debian -- Security Information -- DSA-3000-1 krb5	DEBIAN	w
RT/krbdev.mit.edu: Ticket #7969 Double-free in initiator during SPNEGO renegotiation [CVE-2014-4343]	CONFIRM	k
Mageia Advisory: MGASA-2014-0345 - Updated krb5 package fixes security vulnerabilities	CONFIRM	a
109390	OSVDB	w
IBM X-Force Exchange	XF	e
support.f5.com/kb/en-us/solutions/public/15000/500/sol15553.html	CONFIRM	s
MIT Kerberos Multiple Memory Errors Let Remote Users Deny Service - SecurityTracker	SECTRACK	w
1121876 – (CVE-2014-4343) CVE-2014-4343 krb5: double-free flaw in SPNEGO initiators	CONFIRM	b
[SECURITY] Fedora 20 Update: krb5-1.11.5-10.fc20	FEDORA	li
Fix double-free in SPNEGO [CVE-2014-4343] · krb5/krb5@f18ddf5 · GitHub	CONFIRM	g

Security Advisory SA60082 - SUSE update for krb5 - Secunia	SECUNIA	s
Security Advisory SA60448 - IBM AIX / Virtual I/O Server Kerberos GSSAPI Multiple Vulnerabilities - Secunia	SECUNIA	s
aix.software.ibm.com/aix/efixes/security/nas_advisory1.asc	CONFIRM	a
Security Advisory SA59102 - Debian update for krb5 - Secunia	SECUNIA	s
MIT Kerberos 5: User-assisted execution of arbitrary code (GLSA 201412-53) — Gentoo security	GENTOO	s
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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