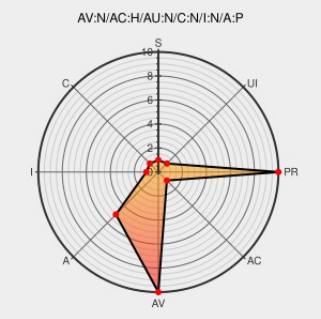
CVE-2013-2139

Published on: 01/15/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-2139

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libsrtp from Cisco contain the following vulnerability:

Buffer overflow in srtp.c in libsrtp in srtp 1.4.5 and earlier allows remote attackers to cause a denial of service (crash) via vectors related to a length inconsistency in the crypto_policy_set_from_profile_for_rtp and srtp_protect functions.

CVE-2013-2139 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 93852
Full Disclosure: [GTA-2013-01] - Libsrtp srtp_protect/hmac_compute buffer overflow	seclists.org text/html	FULLDISC 20130603 [GTA-2013-01] - Libsrtp srtp_protect/hmac_compute buffer overflow
Docupdate by jfigus · Pull Request #27 · cisco/libsrtp · GitHub	github.com text/html	CONFIRM github.com/cisco/libsrtp/pull/27
Support / Security / Advisories / / MDVSA-2014:219 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2014:219
openSUSE-SU-2013:1258-1: moderate: srtp	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1258

Debian -- Security Information -- DSA-2840-1 srtp	www.debian.org Depreciated Link text/html	DEBIAN DSA-2840
openSUSE-SU-2014:1250-1: moderate: srtp	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:1250
Fedora alert FEDORA-2013-24153 (libsrtp) [LWN.net]	lwn.net text/html	FEDORA FEDORA-2013-24153
970697 – (CVE-2013-2139) CVE-2013-2139 libsrtp: buffer overflow in application of crypto profiles	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=970697
Mageia Advisory: MGASA-2014-0465 - Updated srtp package fixes security vulnerability	advisories.mageia.org text/html	CONFIRM advisories.mageia.org/MGASA-2014-0465.html

Related QID Numbers

377499 Alibaba Cloud Linux Security Update for libsrtp (ALINUX2-SA-2020:0125)

671055 EulerOS Security Update for libsrtp (EulerOS-SA-2019-2617)

671111 EulerOS Security Update for libsrtp (EulerOS-SA-2019-2706)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Libsrtp	1.0.1	All	All	All
Application	Cisco	Libsrtp	1.0.2	All	All	All
Application	Cisco	Libsrtp	1.0.4	All	All	All
Application	Cisco	Libsrtp	1.0.5	All	All	All
Application	Cisco	Libsrtp	1.0.6	All	All	All
Application	Cisco	Libsrtp	1.3.20	All	All	All
Application	Cisco	Libsrtp	1.4.0	All	All	All
Application	Cisco	Libsrtp	1.4.1	All	All	All
Application	Cisco	Libsrtp	1.4.2	All	All	All
Application	Cisco	Libsrtp	1.4.4	All	All	All
Application	Cisco	Libsrtp	1.0.1	All	All	All
Application	Cisco	Libsrtp	1.0.2	All	All	All
Application	Cisco	Libsrtp	1.0.4	All	All	All
Application	Cisco	Libsrtp	1.0.5	All	All	All
Application	Cisco	Libsrtp	1.0.6	All	All	All
Application	Cisco	Libsrtp	1.3.20	All	All	All
Application	Cisco	Libsrtp	1.4.0	All	All	All

Application	Cisco	Libsrtp	1.4.0	All	All	All
Application	Cisco	Libsrtp	1.4.1	All	All	All
Application	Cisco	Libsrtp	1.4.2	All	All	All
Application	Cisco	Libsrtp	1.4.4	All	All	All
Application	Cisco	Libsrtp	All	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

cpe:2.3:a:cisco:libsrtp:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:libsrtp:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:18:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:18:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:19:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:20:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→