CVE-2018-4013

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

Summary

CVE	CVE-2018-4013
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-19 13:29:00 UTC
Updated	2022-06-07 17:21:00 UTC
Description	An exploitable code execution vulnerability exists in the HTTP packet-parsing functionality of the LIVE555 RTSP server libra

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Live555	Live555 Media Server	0.92	All	All	All
Application	Live555	Live555 Media Server	0.92	All	All	All

References

Reference	Source	Link	Ta
[Live-devel] New LIVE555 version - fixes a potential vulnerability in the RTSP server implementation	MLIST	lists.live555.com	Ma
[SECURITY] [DLA 1582-1] liblivemedia security update	MLIST	lists.debian.org	Ma
TALOS-2018-0684 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	Ex
Debian -- Security Information -- DSA-4343-1 liblivemedia	DEBIAN	www.debian.org	Th
LIVE555 Media Server: Multiple vulnerabilities (GLSA 202005-06) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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**