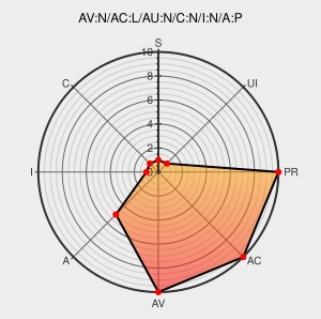
CVE-2013-4926

Published on: 07/29/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-4926

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

epan/dissectors/packet-dcom-sysact.c in the DCOM ISystemActivator dissector in Wireshark 1.10.x before 1.10.1 does not properly determine whether there is remaining packet data to process, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2013-4926 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:17547
8828 – DCOM-SYSACT dissector crash	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8828
Wireshark · wnpa-sec-2013-44 · DCOM ISystemActivator dissector crash	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2013-44.html
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	SECUNIA 54425
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=50478

	text/xml	
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-dcom-sysact.c?r1=50478&r2=50477&pathrev=50478
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-201308-05
Security Advisory SA54296 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 54296
Wireshark · Wireshark 1.10.1 Release Notes	www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.10.1.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→