CVE-2019-12295

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-12295
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-23 12:29:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	In Wireshark 3.0.0 to 3.0.1, 2.6.0 to 2.6.8, and 2.4.0 to 2.4.14, the dissection engine could crash. This was addressed in ep

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	15.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	15.1.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All

Application	F5	Big-ip Application Acceleration Manager	15.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	15.1.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	15.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	15.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	15.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	15.1.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	15.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	15.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All

Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	15.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link	Tags
support.f5.com/csp/article/K06725231	CONFIRM	support.f5.com	
myF5		support.f5.com	
[SECURITY] [DLA 2423-1] wireshark security update	MLIST	lists.debian.org	
Wireshark · wnpa-sec-2019-19 · Wireshark dissection engine crash	MISC	www.wireshark.org	Vendor Advisory
15778 – Buildbot crash output: fuzz-2019-05-11-20211.pcap	MISC	bugs.wireshark.org	Issue Tracking, Patch, Ver
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
support.f5.com/csp/article/K06725231	CONFIRM	support.f5.com	
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org	Patch, Vendor Advisory
USN-4133-1: Wireshark vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Wireshark 'epan/packet.c' Denial of Service Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296089 Oracle Solaris 11.4 Support Repository Update (SRU) 10.1.3 Missing (CPUAPR2019)

501318 Alpine Linux Security Update for wireshark