



CVE-2017-17428

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-17428
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-05 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Cavium Nitrox SSL, Nitrox V SSL, and TurboSSL software development kits (SDKs) allow remote attackers to decrypt TLS

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cavium	Nitrox Ssl Sdk	All	All	All	All
Application	Cavium	Nitrox V Ssl Sdk	All	All	All	All
Application	Cavium	Octeon Sdk	All	All	All	All
Application	Cavium	Octeon Ssl Sdk	All	All	All	All
Application	Cavium	Turbossl Sdk	All	All	All	All
Hardware	Cisco	Ace30 Application Control Engine Module	-	All	All	All
Hardware	Cisco	Ace30 Application Control Engine Module	-	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(2.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.5)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(2.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.5)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(2.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace30 Application Control Engine Module Firmware	3.0(0)a5(3.5)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(2.0)	All	All	All

Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.5)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(2.0)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.5)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(2.0)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.0)	All	All	All
Operating System	Cisco	Ace4710 Application Control Engine Firmware	3.0(0)a5(3.5)	All	All	All
Hardware	Cisco	Ace 4710 Application Control Engine	-	All	All	All
Hardware	Cisco	Ace 4710 Application Control Engine	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5505	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5505	-	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5505 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5505 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5505 Firmware	9.1(7.16)	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5510	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5510	-	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5510 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5510 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5510 Firmware	9.1(7.16)	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5520	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5520	-	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5520 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5520 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5520 Firmware	9.1(7.16)	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5540	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5540	-	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5540 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5540 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5540 Firmware	9.1(7.16)	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5550	-	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5550	-	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5550 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5550 Firmware	9.1(7.16)	All	All	All
Operating System	Cisco	Adaptive Security Appliance 5550 Firmware	9.1(7.16)	All	All	All

Application	Cisco	Webex Conect Im	7.24.1	All	All	All
Application	Cisco	Webex Conect Im	7.24.1	All	All	All
Application	Cisco	Webex Meetings	t31	All	All	All
Application	Cisco	Webex Meetings	t32	All	All	All
Application	Cisco	Webex Meetings	t31	All	All	All
Application	Cisco	Webex Meetings	t32	All	All	All

References

Reference	Source
Cisco Application Control Engine TLS Side Channel Leakage Flaw Lets Remote Users Decrypt TLS Session Data - SecurityTracker	SE
Security Advisory	CC
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	CE
Bleichenbacher Attack on TLS Affecting Cisco Products: December 2017	CI
Multiple Cisco Products Multiple Information Disclosure Vulnerabilities	BI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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