Common Criteria Certification
BSI-DSZ-CC-xyz BSI-CC-PP-00zz

Sicherheitsarchitektur

MAUVECORP MAUVEVPN CLIENT
Version 2.11

MauveCorp
Fliederweg 98
50020 Köln
certification@mauvecorp.com

Dokumentversion 1.0-SNAPSHOT
[Commit 7d63d7c / master]
2020-03-02

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

Dieses Dokument enthält die notwendigen Informationen zur Evaluation der Vertrauenswürdigkeitskomponente ADV_ARC.1 für die Evaluation des MauveCorp MauveVPN Client. Es enthält Informationen zu folgenden Bereichen…

2. Sicherer Start

3. Update des TOE

Der TOE stellt eine dedizierte Funktionalität zum Update des TOE zur Verfügung.

4. Selbstschutz

Die folgenden Kapitel beschreiben die vom TOE getroffenen Maßnahmen, die eine Manipulation durch aktive Entitäten verhindern.

5. Nicht-Umgehbarkeit der Sicherheitsfunktionalität

6. Trennung von Sicherheitsdomänen

7. Härtung des TOE

8. Zuordnung von TSFI zu SFR

TSFI	SFR	Verwendung
LS.LAN.HTTP_MGMT	FPT_TST.1	Aufruf des Selbsttests
	FTP_TRP.1/Admin	Verbindung zur Managemantschnittstelle
LS.LAN.TLS	FCS_CKM.1	Schlüsselaushandlung für TLS
	FCS_CKM.2/TLS	Schlüsselverteilung für TLS
	FCS_CKM.4	TLS Verbindungen im LAN abbauen
	FCS_COP.1/Hash	TLS Hash Operationen
	FCS_COP.1/HMAC	TLS HMAC Operationen
	FCS_COP.1/TLS.AES	TLS Verbindungen
	FCS_COP.1/TLS.Auth	TLS Verbindungen
	FCS_RNG.1/Hash_DRBG	TLS Verbindungen
	FPT_TDC.1/TLS.Zert	TLS Zertifikate prüfen
	FTP_ITC.1/TLS	Sichere Verbindung zur Managemantschnittstelle
LS.WAN.IPSec	FCS_CKM.1	Schlüsselaushandlung für VPN
	FCS_CKM.2/IKE	Schlüsselverteilung für VPN
	FCS_CKM.4	IPSEC Verbindungen im WAN abbauen
	FCS_COP.1/Hash	IPSec Hash Operationen
	FCS_COP.1/HMAC	IPSec HMAC Operationen
	FCS_RNG.1/Hash_DRBG	Schlüsselaushandlung für VPN
	FPT_TDC.1/Zert	VPN Zertifikate prüfen
	FTP_ITC.1/VPN	Sicherer IPSec Tunnel

Weiter auf der nächsten Seite

TSFI	SFR	Verwendung
LS.WAN.NTP	FPT_STM.1	Zugang zum Zeitdienst
Keine TSFI	FDP_RIP.1	Sicheres Löschen nicht von außen aufrufbar

Tabelle 8.1.: Zuordnung von TSFI zu SFR

A. TLS Verbindungen

Für die TLS-Verbindungen werden die im Schutzprofil genannten Cipher Suiten verwendet. Der TOE beherrscht genau diese Cipher Suiten und keine darüber hinaus. Tabelle A.1 listet diese Cipher Suiten auf. Tabelle A.2 zeigt die elliptischen Kurven, die beim ECDHE Schlüsselaustausch zur Anwendung kommen.

Algorithmen / Cipher Suite	IANA ID	TLS 1.2 [RFC 5246]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	`0x00,0x33`	✓
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	`0x00,0x39`	✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	`0xc0,0x13`	✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	`0xc0,0x14`	✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	`0xc0,0x27`	✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	`0xc0,0x28`	✓
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	`0xc0,0x2f`	✓
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	`0xc0,0x30`	✓

Tabelle A.1.: Cipher Suites der TLS Verbindungen des TOE

Elliptische Kurve	IANA ID	Standard
secp256r1 (P-256)	`23`	[RFC 8422; ANSI X9.62]
secp384r1 (P-384)	`24`	[RFC 8422; ANSI X9.62]
brainpoolP256r1	`26`	[RFC 7027]
brainpoolP384r1	`27`	[RFC 7027]

Tabelle A.2.: Elliptische Kurven für die TLS Verbindungen des TOE

Der TOE kommuniziert mit anderen vertrauenswürdigen IT-Produkten über gesicherte Verbindungen. Die Integrität und die Vertrauenswürdigkeit der Verbindungen wird durch die Verwendung von TLS in der Version 1.2 und die in Tabelle A.1 genannten Algorithmen und Cipher Suiten sichergestellt. Tabelle A.4 listet die Verbindungen auf, die der TOE eingeht. Die Spalten dieser Tabelle werden in Tabelle A.3 beschrieben.

Spalte	Beschreibung
ID	Symbolischer Name der Verbindung
Schnittstelle	Logische Schnittstelle, deren Kommunikation abgesichert wird.
Rolle	Beschreibt, ob der TOE in dieser Verbindung Client oder Server ist.
Peer	Beschreibung des Partners in der TLS-Verbindung
Protokoll	Anwendungsprotokoll, das für die Verbindung genutzt wird.
Subsystem::Modul	Name des Subsystems und des Moduls, von dem die Verbindung ausgeht, bzw. das die Verbindung empfängt und behandelt.
Port	Port, den der TOE öffnet, um die Verbindung aufzubauen. Für Verbindungen, bei denen der TOE Server ist, steht hier eine Portnummer. Wenn der TOE Client ist, steht „dyn.“ für die ephemerische Portvergabe bei TCP-Verbindungen. „konfig.“ steht dafür, dass der Zielport konfigurierbar ist.
Schnittstelle	Logische Schnittstelle des TOE , über die die Verbindung läuft.
Identität des TOE	Zertifikat, mit dem sich der TOE gegenüber dem Peer authentisiert.
Identität des Peer	Zertifikat/Verfahren, mit dem sich der Peer gegenüber dem TOE authentisiert.
Authentifizierung des Peer durch	Verfahren, Datenquelle oder Subsystem/Modul, mit dem der TOE die Identität des Peers verifiziert.

Tabelle A.3.: Legende zu den TLS Verbindungen

ID	Schnittstelle (Protokoll)	Rolle	Peer	Subsystem::Modul	Port	Identität des TOE	Identität des Peer	Authentifizierung des Peer durch
TLS.1	LS.LAN.HTTP_MGMT	Server	Browser	Administrationssystem::HTTP-Server	443	Zertifikat aus Mauve CA	Benutzername/Passwort	Benutzerverwaltung im TOE

Tabelle A.4.: TLS Verbindungen des MauveVPN Client

B. Liste der TSFI

Der TOE verfügt über die logischen Schnittstellen, die das Schutzprofil [BSI-CC-PP-00zz] beschreibt. Diese werden hier der besseren Lesbarkeit halber wiederholt.

LS.LAN ist die Schnittstelle des TOE ins lokale Netzwerk der Einsatzumgebung. Zusätzlich zu den im Schutzprofil genannten Schnittstellen werden hier weitere protokollspezifische Schnittstellen definiert. Tabelle B.1 listet diese logischen Schnittstellen.

LS.WAN ist die Schnittstelle des TOE zum WA. Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung des WAN. Tabelle B.2 listet diese logischen Schnittstellen.

LS.LED repräsentiert die logische Schnittstelle zum Display und den Bedienknöpfen über PS.LED.

Bezeichner	Rolle	Zweck der Schnittstelle
LS.LAN.Ether	—	Protokoll auf Zugangsschicht
LS.LAN.IP	—	Zugang zur Internet-Schicht
LS.LAN.TCP	—	Zugang zur Transportschicht
LS.LAN.TLS	beide	Sicherung der Verbindung mit TLS 1.2
LS.LAN.UDP	—	Zugang zur Transportschicht
LS.LAN.HTTP_MGMT	Server	HTTP-Zugriff auf Managementschnittstelle

Tabelle B.1.: Logische Schnittstellen an LS.LAN

Bezeichner	Rolle	Zweck der Schnittstelle
LS.WAN.Ether	—	Protokoll auf Zugangsschicht
LS.WAN.IP	—	Zugang zur Internet-Schicht
LS.WAN.NTP	Client	Abruf der Uhrzeit
LS.WAN.DHCP	Client	Adressbezug im WAN
LS.WAN.TCP	—	Zugang zur Transportschicht
LS.WAN.UDP	—	Zugang zur Transportschicht
LS.WAN.IPSec	—	VPN Datenverkehr

Tabelle B.2.: Logische Schnittstellen an LS.WAN

Literatur

[ANSI X9.62] Accredited Standards Committee X9. *ANSI X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Standard. ANSI, 16. Nov. 2005.

[BSI-CC-PP-00zz] Bundesamt für Sicherheit in der Informationstechnik. *Schutzprofil: Anforderungen an den VPN Client. BSI-CC-PP-00zz*. Common Criteria Schutzprofil (Protection Profile). Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), 5. Feb. 2020.

[RFC 5246] T. Dierks und E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246 (Proposed Standard). RFC. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905, 7919. Fremont, CA, USA: RFC Editor, Aug. 2008. DOI: 10.17487/RFC5246. URL: https://www.rfc-editor.org/rfc/rfc5246.txt.

[RFC 7027] J. Merkle und M. Lochter. *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)*. RFC 7027 (Informational). RFC. Fremont, CA, USA: RFC Editor, Okt. 2013. DOI: 10.17487/RFC7027. URL: https://www.rfc-editor.org/rfc/rfc7027.txt.

[RFC 8422] Y. Nir, S. Josefsson und M. Pegourie-Gonnard. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. RFC 8422 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2018. DOI: 10.17487/RFC8422. URL: https://www.rfc-editor.org/rfc/rfc8422.txt.