Mauve Corp

Fictional but secure products

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

Sicherheitsarchitektur

MAUVECORP MAUVEVPN CLIENT
Version 2.11

MauveCorp
Fliederweg 98
D-50020 Köln
certification@mauvecorp.com

Dokumentversion 1.0-SNAPSHOT
13.09.2022
[Commit cc54422 / main]

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
LI.LAN.HTTP_MGMT	FPT_TST.1	Call self-test
	FTP_TRP.1/Admin	Connection to management interface
LI.LAN.TLS	FCS_CKM.1	Key negotiation for TLS
	FCS_CKM.2/TLS	Key distribution for TLS
	FCS_CKM.4	Terminate TLS connections to LAN
	FCS_COP.1/Hash	TLS hash operations
	FCS_COP.1/HMAC	TLS HMAC operations
	FCS_COP.1/TLS.AES	TLS connections
	FCS_COP.1/TLS.Auth	TLS connections
	FCS_RNG.1/Hash_DRBG	TLS connections
	FPT_TDC.1/TLS.Zert	Validate TLS certificate
	FTP_ITC.1/TLS	Secure connection to management interface
LI.WAN.IPSec	FCS_CKM.1	Key negotiation for VPN
	FCS_CKM.2/IKE	Key distribution for VPN
	FCS_CKM.4	Terminate IPSEC connections to WAN
	FCS_COP.1/Hash	IPSec hash operations
	FCS_COP.1/HMAC	IPSec HMAC operations
	FCS_RNG.1/Hash_DRBG	Key negotiation for VPN
	FPT_TDC.1/Zert	Validate VPN certificate
	FTP_ITC.1/VPN	Secure IPSec tunnel

Weiter auf der nächsten Seite

TSFI	**SFR**	Verwendung
LI.WAN.NTP	FPT_STM.1	Access to time service
Keine TSFI	FDP_RIP.1	Not accessible via TSFI

Tabelle 8.1.: Zuordnung von TSFI zu SFR

A. TLS Connections

The Protection Profiles defines the cipher suites required for TLS connections. The TOE uses provides exactly those cipher suites and no other. Tabelle A.1 lists these cipher suites. Tabelle A.2 lists the elliptic curves used for ECDHE.

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 for TLS connections

Elliptic curve	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.: Elliptic curves for TLS connections

The TOE communicates with other trusted IT products over secure connections. Integrity and confidentiality of these connections is ensured by TLS v1.2. Tabelle A.4 lists all connections the TOE can participate in. Tabelle A.3 describes the columns of this table.

Column	Descriptions
ID	Smybolic name of this connection
Interface	Logical interface whose communication is secured.
Role	Describes client/serer role of the TOE.
Peer	Describes the peer in this TLS connection.
Protocol	Application protocol used in this connection.
Subsystem::Module	Name of the subsystem and the module from which the connection originates or that accepts the connections.
Port	IP-Port that the TOE opens for the connection. If the TOE is client, “dyn.” stands for ephemeral port assignment. “config” stands for a confgurable port number.
Identity of TOE	Certificate that the TOE uses to authenticate itself to the peer.
Identity of Peer	Certificate that the peer uses to authenticate itself to the TOE.
Authentication by	Process, data source or subsystem/module used by the TOE for authentication/verification.

Tabelle A.3.: Legend for TLS connections

ID	Interface (protocol)	Role	Peer	Subsystem::Module	Port	Identity of TOE	Identity of Peer	Authentication by
TLS.1	LI.LAN.HTTP_MGMT	Server	Browser	Administration::HTTP-Server	443	Certificate from Mauve CA	Username/password	User administration in TOE

Tabelle A.4.: TLS connections of MauveVPN Client

B. List of TSFI

The TOE provides the logical interfaces described in the protection profile [BSI-CC-PP-00zz]. They are repeated here.

LS.LAN is the TOE's interface to the local area network of the operating environment. In addition to the interfaces described in the protection profile, there are further protocol specific interfaces described here. Tabelle B.1 lists these logical interfaces.

LS.WAN is the TOE's interface to the wide area network of the operating environment, the Internet. In addition to the interfaces described in the protection profile, there are further protocol specific interfaces described here. Tabelle B.2 lists these logical interfaces.

LS.LED represents the logical interface to the display and the buttons of PS.LED.

Label	Client/Server	Purpose of the interface
LI.LAN.Ether	—	media access
LI.LAN.IP	—	access to the Internet layer
LI.LAN.TCP	—	access to the transport layer
LI.LAN.TLS	server	transport security with TLS 1.2
LI.LAN.UDP	—	access to the transport layer
LI.LAN.HTTP_MGMT	server	HTTP access to the management console

Tabelle B.1.: Logical Interfaces on LI.LAN

Label	Client/Server	Purpose of the interface
LI.WAN.Ether	—	media access
LI.WAN.IP	—	access to the Internet layer
LI.WAN.TCP	—	access to the transport layer
LI.WAN.NTP	client	Obtaining time
LI.WAN.DHCP	client	Obtaining IP addresses in the WAN
LI.WAN.UDP	—	access to the transport layer
LI.WAN.IPSec	—	VPN data traffic

Tabelle B.2.: Logical Interfaces on LI.WAN

Literatur

Schutzprofile und Technische Richtlinien

[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.

Standards

[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.

RFC

[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.