National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Fortra’s GoAnywhere Managed File Transfer v6.8

Report Number:	**CCEVS-VR-VID11216-2023**
Dated:	**04/07/2023**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
Attn: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D. Lead Validator

Jerome Myers, Ph.D. Senior Validator

The Aerospace Corporation

Common Criteria Testing Laboratory

George Kumi

Sai Sandeep Yanamandra

Shaunak Shah

Acumen Security, LLC

Table of Contents

1 Executive Summary 4

2 Identification 6

3 Architectural Information 8

4 Security Policy 9

4.1 Cryptographic Support 9
4.2 User Data Protection 10
4.3 Identification and Authentication 10
4.4 Security Management 11
4.5 Privacy 11
4.6 Protection of the TSF 11
4.7 Trusted Path/Channels 11

5 Assumptions, Threats & Clarification of Scope 12

5.1 Assumptions 12
5.2 Threats 12
5.3 Clarification of Scope 13

6 Documentation 14

7 TOE Evaluated Configuration 15

7.1 Evaluated Configuration 15

8 IT Product Testing 17

8.1 Developer Testing 17
8.2 Evaluation Team Independent Testing 17

9 Results of the Evaluation 18

9.1 Evaluation of Security Target 18
9.2 Evaluation of Development Documentation 18
9.3 Evaluation of Guidance Documents 19
9.4 Evaluation of Life Cycle Support Activities 19
9.5 Evaluation of Test Documentation and the Test Activity 19
9.6 Vulnerability Assessment Activity 20
9.7 Summary of Evaluation Results 28

10 Validator Comments & Recommendations 30

11 Annexes 31

12 Security Target 32

13 Glossary 33

14 Bibliography 34

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Fortra's GoAnywhere Managed File Transfer v6.8 (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in April 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP].

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP]. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Fortra's GoAnywhere Managed File Transfer v6.8
Protection Profile	Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP] Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP]
Security Target	Fortra's GoAnywhere Managed File Transfer v6.8 Security Target v 1.1
Evaluation Technical Report	Evaluation Technical Report for Fortra's GoAnywhere Managed File Transfer v6.8, 1.1, 31 March 2023
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Fortra, LLC
Developer	Fortra, LLC

Item	Identifier
Common Criteria Testing Lab (CCTL)	Acumen Security LLC Rockville, MD 20850
CCEVS Validators	Patrick Mallett: Lead Validator Jerome Myers: Senior Validator

3 Architectural Information

The Target of Evaluation (TOE) is the Fortra's GoAnywhere Managed File Transfer v6.8 (MFT). The TOE is a software application that provides secure file transfer services over HTTPS, TLS, and SSH. GoAnywhere MFT is a secure managed file transfer solution that streamlines the exchange of data between systems, employees, customers, and trading partners. It provides centralized control with extensive security settings, detailed audit trails, and helps process information from files into XML, CSV, and JSON databases.

4 Security Policy

The TOE provides the security functionality required by [SWAPP], [TLS-PKG], and [SSH-EP].

4.1 Cryptographic Support

The TOE utilizes the GoAnywhere MFT Bouncy Castle FIPS Java API cryptographic library version 1.0.2. This library implements all of the cryptographic algorithms required for SSH and TLS, drawing entropy from the platform RBG.

The cryptographic services provided by the TOE are described below.

Table 2 TOE Provided Cryptography

Cryptographic Protocol	Use within the TOE
SSHv2 Client	File server transfers using SFTP or SCP
SSHv2 Server	User file transfers using SFTP or SCP
HTTPS/TLSv1.2 Client	File server transfers using AS2, AS4, WebDAV, FTP/s, Amazon S3, Azure Blob Storage, REST, SOAP, or HTTPS; Check for updates
HTTPS/TLSv1.2 Server	HTTPS Remote administration; HTTPS file access; AS2 or AS4 clients
TLSv1.2 Client	Database server; Authentication Server; Mail Server;
TLSv1.2 Server	User file transfers using FTP/s

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Table 3 CAVP Algorithm Testing References

SFR	Algorithm in ST	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3	RSA KeyGen (n = 2048, 3072)	C1876
	ECC schemes using “NIST curves” [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4	ECDSA KeyGen ECDSA KeyVer (Curve = P-256, P-384, P-521)	C1876
	FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3	NIAP Policy Letter #5, Addendum #2, states “No NIST CAVP, CCTL must perform all assurance/evaluation activities”.	Vendor Affirmed.
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-	NIAP Policy Letter #5, Addendum #2, states “No NIST CAVP exists, must be described	Vendor Affirmed.

SFR	Algorithm in ST	CAVP Alg.	CAVP Cert #
	Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"	in TSS – See FIPS 140-2 I.G. D.4: Vendor Affirmation".	
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	KAS-ECC (Curve = P-256, P-384, P-521)	C1876
	Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3	NIAP Policy Letter #5, Addendum #2 does not provide any guidance for this selection.	Vendor Affirmed.
FCS_COP.1/ DataEncryption	AES used in [**CBC, GCM**] mode and cryptographic key sizes [**128 bits, 256 bits**]	AES-CBC (128-bit, 256-bit) AES-GCM (128-bit, 256-bit)	C1876
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	RSA SigGen RSA SigVer (n = 2048, 3072)	C1876
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [**P-256, P-384, P-521**]; ISO/IEC 14888-3, Section 6.4	ECDSA SigGen ECDSA SigVer (Curve = P-256, P-384, P-521)	C1876
FCS_COP.1/ Hash	[**SHA-1, SHA-256, SHA-384, SHA-512**] and message digest sizes [**160, 256, 384, 512**] bits	SHA-1 SHA2-256 SHA2-384 SHA2-512	C1876
FCS_COP.1/ KeyedHash	[**HMAC-SHA-1, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512**] and cryptographic key sizes [**256-bits, 160-bits, 384-bits, 512-bits**] and message digest sizes [**160, 384, 512**] bits	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	C1876
FCS_RBG_EXT.1	**CTR_DRBG (AES)**	Counter DRBG (AES)	C1876

4.2 User Data Protection

The TOE relies on the underlying platform to encrypt sensitive data at rest.

4.3 Identification and Authentication

The TOE uses X.509v3 certificates as defined by RFC 5280 to authenticate the TLS connection to the external TLS servers. The TOE validates the X.509 certificates using the certificate path validation algorithm defined in RFC 5280.

The TOE authenticates users using a username/password combination or X.509 TLS Client Certificates.

4.4 Security Management

The TOE allows the configuration of users, file servers, file transfer services, keys and certificates, and cryptographic protocols.

4.5 Privacy

The TOE does not transmit Personally Identifiable Information (PII) over the network.

4.6 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE only allocates a limited amount of memory with both write and execute permission to support just-in-time compiling. The TOE supports ASLR, stack-based overflow protections, and platform security mechanisms (Windows Defender and SELinux).

The TOE is distributed as a Microsoft .EXE file (Windows) or a RPM (CentOS). The installers are signed by Fortra so their integrity can be verified by the platform.

4.7 Trusted Path/Channels

The TOE protects all data in transit using TLSv1.2 or SSHv2.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The following assumptions are drawn directly from the SWAPP.

Table 4 Assumptions

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

The following threats are drawn directly from the SWAPP.

Table 5 Threats

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

ID	Threat
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP].
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Fortra's GoAnywhere Managed File Transfer v6.8 Common Criteria Configuration Guide, Version 1.1 [AGD]

Only the Configuration Guide listed above and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration."

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the following Fortra's GoAnywhere Managed File Transfer v6.8 software application running on the following platforms when configured in accordance with the documentation specified in section 6.

- CentOS 7 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)
- Windows Server 2016 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)

Note: The TOE is the application software only. The host platforms are not part of the evaluation.

The TOE supports (sometimes optionally) secure connectivity with several other IT environment devices as described below.

Table 6 IT Environment Components

Environment Component	Required	Usage/Purpose Description
Web Browser	Yes	Remote administration and User file access over HTTPS/TLSv1.2.
Database Server	Yes	MySQL, PostgreSQL, MS SQL Server, Oracle, or DB2/400 for storing settings. The server must support TLSv1.2 to enable secure access by the TOE.
LDAP/AD Server	No	Remote authentication server supporting TLSv1.2.
Mail Server	No	Mail server supporting SMTP over TLSv1.2 for sending notifications.
File Server	No	Remote file server for storing user files: • AS2, AS4, or WebDAV servers supporting HTTPS/TLSv1.2 • SFTP or SCP servers supporting SSHv2 • FTP/s servers supporting TLSv1.2 • Amazon S3 or Azure Blob Storage supporting HTTPS/TLSv1.2 • REST, SOAP, or generic HTTPS/TlSv1.2 server
File Transfer Client	No	Client allowing users to store and retrieve files from the TOE: • AS2 or AS4 clients supporting HTTPS/TLSv1.2 • SFTP or SCP clients supporting SSHv2 • FTP/s client supporting TLSv1.2
Java Runtime Environment	Yes (on CentOS)	Platform-provided Java SE 8 Java Runtime Environment (JRE). Note: The Windows platform does not provide a JRE, so the Windows version of the TOE includes the required JRE.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Fortra's GoAnywhere Managed File Transfer v6.8, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Fortra's GoAnywhere Managed File Transfer v6.8 to be Part 2 and Part 3 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the AppSW, TLS-PKG and SSH-EP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Fortra's GoAnywhere Managed File Transfer v6.8 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP].

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The following was performed on January 15, 2023, and then repeated on March 29, 2023.

The evaluator searched the Internet for potential vulnerabilities in the Product using the web sites listed below. The sources of the publicly available information are provided below.

- https://www.goanywhere.com
- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/
- https://www.cvedetails.com/

The following components of the Product were searched:

Component	CPE
fortra	cpe:2.3:a:fortra
helpsystems 6.6.0	cpe:2.3:a:helpsystems:boks:6.6.0:*:*:*:*:*:*:*
helpsystems 6.7.1	cpe:2.3:a:helpsystems:boks:6.7.1:*:*:*:*:*:*:*
helpsystems 6.8.7	cpe:2.3:a:goanywhere:mft:6.8.7:*:*:*:*:*:*:*
goanywhere	cpe:2.3:a:goanywhere:*:*:*:*:*:*:*
GoAnywhere MFT Bouncy Castle FIPS Java API	cpe:2.3:a:GoAnywhereMFTBouncyCastleFIPSJavaAPI:*:*:*:*:*:*:*
centos 7.0	cpe:2.3:o:centos:centos:7.0:*:*:*:*:*:*:*
intel xeon e5-4620 v4	cpe:2.3:h:intel:xeon_e5-4620_v4:-:*:*:*:*:*:*:*
Azul Zulu Java SE 8 Update 272	cpe:2.3:a:azul:zulu:8:update272:*:*:*:*:*:*
vmware esxi 6.7	cpe:2.3:o:vmware:esxi:6.7:-:*:*:*:*:*:*
all-themes-1.0.8.jar	cpe:2.3:a:all-themes-1.0.8.jar:*:*:*:*:*:*:*
apache tomcat 9:0:41	cpe:2.3:a:apache:tomcat:9.0.41:*:*:*:*:*:*:*
apache-mime4j-core-0.7.2	cpe:2.3:a:apache:mime4j:core-0.7.2:*:*:*:*:*:*:*
aws-java-sdk-cloudfront	cpe:2.3:a:amazon:aws_sdk_for_cloudfront:-:*:*:*:*:node.js:*:*

aws-java-sdk-core-1.11.631	cpe:2.3:a:amazon:aws_sdk_for_core:1.11.631:*:*:*:*:node.js:*:*
aws-java-sdk-kms-1.11.631	cpe:2.3:a:amazon:aws_sdk_for_kms:1.11.631:*:*:*:*:node.js:*:*
aws-java-sdk-s3-1.11.631	cpe:2.3:a:amazon:aws_s3_crypto_sdk:1:*:*:*:*:golang:*:*
aws-java-sdk-sts-1.11.631	cpe:2.3:a:amazon:aws_java_sdk_sts:1:*:*:*:*:golang:*:*
azure storage 5.5.0	cpe:2.3:a:azure:storage:5.5.0:*:*:*:*:*:*:*
apache batik 1.10	cpe:2.3:a:apache:batik:1.10:*:*:*:*:*:*:*
bouncy castle fips 1.0.2	cpe:2.3:a:bouncycastle:fips_java_api:1.0.2:*:*:*:*:*:*:*
bouncy castle mail fips 1.0.3	cpe:2.3:a:bouncycastle:mail:fips:1.0.3:*:*:*:*:*:*
bouncy castle pg fips 1.0.5	cpe:2.3:a:bouncycastle:pg:fips:1.0.5:*:*:*:*:*:*
bouncy castle cryptography APIs	cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.02:*:*:*:*:*:*:*
bctls fips 1.0.10.3	cpe:2.3:a:bouncycastle:tls:fips:1.0.10.3:*:*:*:*:*:*
bluesky 1.0.6	cpe:2.3:a:bluesky:1.0.6:*:*:*:*:*:*
bsh-2.0b6	cpe:2.3:a:beanshell:beanshell:2.0:beta6:*:*:*:*:*:*
chartcreator-1.2.0	cpe:2.3:a:chartcreator:1.2.0:*:*:*:*:*:*
commons_beanutils 1.9.4	cpe:2.3:a:apache:commons_beanutils:1.9.4:*:*:*:*:*:*:*
commons-cli 1.3.1	cpe:2.3:a:apache:commons-cli:1.3.1:*:*:*:*:*:*:*
commons-codec 1.14	cpe:2.3:a:apache:commons-codec:1.14:*:*:*:*:*:*:*
commons collections 3.2.2	cpe:2.3:a:apache:commons_collections:3.2.2:*:*:*:*:*:*:*
commons collections 4.4.1	cpe:2.3:a:apache:commons_collections:4.4.1:*:*:*:*:*:*:*

commons compress 1.19	cpe:2.3:a:apache:commons_compress:1.19:*:*:*:*:*:*:*
commons configuration 1.7	cpe:2.3:a:apache:commons_configuration:1.7:*:*:*:*:*:*:*
commons dbcp 1.3	cpe:2.3:a:apache:commons:dbcp:1.3:*:*:*:*:*:*
commons digestoer 1.8.1	cpe:2.3:a:apache:commons:digester:1.8.1:*:*:*:*:*:*
commons discovery 0.4	cpe:2.3:a:apache:commons:discovery:0.4:*:*:*:*:*:*
commons-el	cpe:2.3:a:apache:commons:el:*:*:*:*:*:*
commons fileupload 1.4	cpe:2.3:a:apache:commons_fileupload:1.4:*:*:*:*:*:*:*
commons httpclient 3.0	cpe:2.3:a:apache:commons-httpclient:3.0:*:*:*:*:*:*:*
commons-io 2.6	cpe:2.3:a:apache:commons-io:2.6:*:*:*:*:*:*:*
commons-lang 2.1	cpe:2.3:a:apache:commons-lang:2.1:*:*:*:*:*:*:*
commons-lang3 3.9	cpe:2.3:a:apache:commons-lang3:3.9:*:*:*:*:*:*:*
commons logging 1.2	cpe:2.3:a:apache:commons-logging:1.2:*:*:*:*:*:*:*
commons math3 3.6.1	cpe:2.3:a:apache:commons-math3:3.6.1:*:*:*:*:*:*:*
commons-net-3.3.0	cpe:2.3:a:netcommons:netcommons:3.3.0:*:*:*:*:*:*:*
commons-pool-1.6	cpe:2.3:a:apache:commons-pool:1.6:*:*:*:*:*:*:*
commons-validator-1.5.0	cpe:2.3:a:apache:commons-validator:1.5.0:*:*:*:*:*:*:*
commons-vfs2-2.1	cpe:2.3:a:apache:commons-vfs2:2.1:*:*:*:*:*:*:*
cryptojce	cpe:2.3:o:cryptojce:*:*:*:*:*:*:*
cryptojcommon	cpe:2.3:o:cryptojcommon:*:*:*:*:*:*:*
css parser	cpe:2.3:a:horde:horde_css_parser:1.0.0:*:*:*:*:*:*:*
curvesapi 1.0.6	cpe:2.3:o:curvesapi:1.0.6:*:*:*:*:*:*:*
db2jcc	cpe:2.3:a:ibm:db2:11.1:*:*:*:*:*:*:*

derby	cpe:2.3:a:apache:derby:-:*:*:*:*:*:*:*
derby client	cpe:2.3:a:apache:derby:client:*:*:*:*:*:*:*
ehcache-core-2.5.1	cpe:2.3:a:ehcache:core:2.5.1:*:*:*:*:*:*:*
esapi-2.1.0.1	cpe:2.3:a:owasp:enterprise_security_api:2.1.0.1:*:*:*:*:*:*:*
facestrace 0.9.0	cpe:2.3:a:facestrace:0.9.0:*:*:*:*:*:*:*
face info set	cpe:2.3:a:faceinfoset:*:*:*:*:*:*:*
font awesome 5.6.1	cpe:2.3:a:font:awesome:5.6.1:*:*:*:*:*:*:*
gmbal-api-only	cpe:2.3:a:oracle:glassfish:-:*:*:*:*:*:*:*
gson 2.2.4	cpe:2.3:a:gson:2.2.4:*:*:*:*:*:*:*
guava 26.0	cpe:2.3:a:google:guava:26.0:*:*:*:*:*:*:*
ha-api	cpe:2.3:a:ha:api:*:*:*:*:*:*:*
httpclient 4.5.13	cpe:2.3:a:apache:httpclient:4.5.13:*:*:*:*:*:*:*
httpcore 4.4.14	cpe:2.3:a:apache:httpcore:4.4.14:*:*:*:*:*:*:*
icu4j-63.1	cpe:2.3:a:icu-project:international_components_for_unicode:63.1:*:*:*:*:c\/c\+\+:*:*
ifxjdbc	cpe:2.3:a:ibm:informix_jdbc:*:*:*:*:*:*:*
imagscalr-lib 4.2	cpe:2.3:a:imgscalr:lib:4.2:*:*:*:*:*:*:*
ion-java-1.0.2	cpe:2.3:a:amazon:ion:1.02:*:*:*:*:node.js:*:*
ipworkszip	cpe:2.3:a:ipworkszip:*:*:*:*:*:*:*
itext 2.1.7	cpe:2.3:a:itextpdf:itext:2.1.7:*:*:*:*:*:*:*
jackson annotations	cpe:2.3:a:fasterxml:jackson:2.10.0:*:*:*:*:*:*:*
jackson core	cpe:2.3:a:fasterxml:jackson-core:*
jackson databind 2.10.5	cpe:2.3:a:fasterxml:jackson-databind:2.10.5:*:*:*:*:*:*:*

jakartha oro	cpe:2.3:a:jakartha:oro:*:*:*:*:*:*:*
jasperreports 6.7.1	cpe:2.3:a:jaspersoft:jasperreports:6.7.1:*:*:*:*:*:*:*
jasperreports-chart-themes 6.7.0	cpe:2.3:a:jaspersoft:jasperreports-chart-themes:6.7.0:*:*:*:*:*:*:*
jasperreports-fonts 6.7.1	cpe:2.3:a:jaspersoft:jasperreports-fonts:6.7.1:*:*:*:*:*:*:*
jasypt 1.9.2	cpe:2.3:a:jasypt_project:jasypt:1.9.2:*
java jwt 3.3.0	cpe:2.3:a:java:jwt:3.3.0:*:*:*:*:*:*:*
javax annotation	cpe:2.3:a:oracle:javax:annotation:*:*:*:*:*:*:*
java xml soap	cpe:2.3:a:javax:xml:soap:*:*:*:*:*:*:*
jaxb-api	cpe:2.3:o:jaxb-api:*:*:*:*:*:*:*
jaxb core	cpe:2.3:o:jaxb-core:*:*:*:*:*:*:*
jaxb-impl	cpe:2.3:o:jaxb-impl:*:*:*:*:*:*:*
jaxb-jxc	cpe:2.3:o:jaxb-jxc:*:*:*:*:*:*:*
jaxb-xjc	cpe:2.3:o:jaxb-xjc:*:*:*:*:*:*:*
jaxws-rt	cpe:2.3:o:jaxws-rt:*:*:*:*:*:*:*
jaxws-tools	cpe:2.3:o:jaxws-tools:*:*:*:*:*:*:*
jcifs 1.3.18	cpe:2.3:o:jcifs:1.3.18:*:*:*:*:*:*:*
jcmFIPS	cpe:2.3:a:oracle:jcmFIPS:*:*:*:*:*:*:*
jcommon-1.0.10	cpe:2.3:a:oracle:jcommon:1.0.10:*:*:*:*:*:*:*
jfreechat 1.0.19	cpe:2.3:a:oracle:jfreechart:1.0.19:*:*:*:*:*:*:*
jgroups 4.1.2	cpe:2.3:a:jgroups:jgroup:4.1.2:*:*:*:*:*:*:*
jmespath java 1.11.631	cpe:2.3:a:amazon:jmespath:java:1.11.631:*:*:*:*:*:*
jms	cpe:2.3:a:jenkins:jms_messaging:1.1.1:*:*:*:*:jenkins:*:*

jnq 1.3.6	cpe:2.3:o:jnq:1.3.6:*:*:*:*:*:*:*
joda-time 2.2	cpe:2.3:o:joda-time:2.2:*:*:*:*:*:*:*
jsch 0.1.54	cpe:2.3:o:jsch:0.1.54:*:*:*:*:*:*:*
jsr181 api	cpe:2.3:a:jsr181:*:*:*:*:*:*
jt400	cpe:2.3:a:jt400:*:*:*:*:*:*
jTDS3	cpe:2.3:a:jTDS3:*:*:*:*:*:*
jxl	cpe:2.3:a:jxl:*:*:*:*:*:*
jzlib 1.1.2	cpe:2.3:a:jcraft:jzlib:1.1.2:*:*:*:*:*:*:*
log4j 1.2	cpe:2.3:a:apache:log4j:1.2:-:*:*:*:*:*:*
log4j-1.2-api-2.13.3	cpe:2.3:a:apache:log4j:2.13.3:rc1:*:*:*:*:*:*
log4j-core 2.13.3	cpe:2.3:a:apache:log4j-core:2.13.3:rc1:*:*:*:*:*:*
log4j-slf4j-impl-2.13.3	cpe:2.3:a:slf4j:slf4j-log4j-2:13.3:*:*:*:*:*:*:*
lucene analyzers common 4.7.2	cpe:2.3:a:apache:lucene-analyzers:common:4.7.2*:*:*:*:*:*:*
lucene codecs 4.7.2	cpe:2.3:a:apache:lucene-codecs:4.7.2*:*:*:*:*:*:*
lucene core 4.7.2	cpe:2.3:a:apache:lucene-core:4.7.2*:*:*:*:*:*:*
lucene-grouping 4.7.2	cpe:2.3:a:apache:lucene-grouping:4.7.2*:*:*:*:*:*:*
lucene-queries 4.7.2	cpe:2.3:a:apache:lucene-queries:4.7.2*:*:*:*:*:*:*
lucene-queryparser 4.7.2	cpe:2.3:a:apache:lucene-queryparser:4.7.2*:*:*:*:*:*:*
management-api	cpe:2.3:a:management-api:*:*:*:*:*:*
mariadb-java-client 1.7.1	cpe:2.3:a:mariadb-java-client:1.7.1:*:*:*:*:*:*:*
maverick-legacy-server 1.7.34	cpe:2.3:a:maverick-legacy-server:1.7.34:*:*:*:*:*:*:*

mimepull	cpe:2.3:a:mimepull:*:*:*:*:*:*:*
mina-core 2.1.4	cpe:2.3:a:apache:mina:2.1.4:*:*:*:*:*:*:*
msbase	cpe:2.3:a:msbase:*:*:*:*:*:*:*
mssqlserver	cpe:2.3:a:mssqlserver:*:*:*:*:*:*:*
msutil	cpe:2.3:a:msutil:*:*:*:*:*:*:*
myfaces 2.2.12	cpe:2.3:a:apache:myfaces:2.2.12:*:*:*:*:*:*:*
native-lib-loader 2.0.2	cpe:2.3:a:native-lib-loader:2.0.2:*:*:*:*:*:*:*
netty 4.1.48	cpe:2.3:a:netty:netty:4.1.48:*:*:*:*:*:*:*
not going to be common ssl 0.3.18	cpe:2.3:a:not-going-to-be-common:ssl:0.3.18*:*:*:*:*:*:*
ojdbc5	cpe:2.3:a:ojdbc5:*:*:*:*:*:*:*
opensaml 2.6.6	cpe:2.3:a:shibboleth:opensaml:2.6.6:*:*:*:*:*:*:*
openws 1.5.4	cpe:2.3:a:shibboleth:openws:1.5.4:*:*:*:*:*:*:*
oro 2.0.8	cpe:2.3:a:jahia:oro:2.0.8:*:*:*:*:*:*:*
owasp sanitizer	cpe:2.3:a:owasp:json-sanitizer:*:*:*:*:*:*:*:*
poi 4.1.1	cpe:2.3:a:apache:poi:4.1.1:*:*:*:*:*:*:*
poi ooxml 4.1.1	cpe:2.3:a:apache:poi-ooxml:4.1.1:*:*:*:*:*:*:*
poi ooxml schemas 4.4.1	cpe:2.3:a:apache:poi-ooxml-schemas:4.1.1:*:*:*:*:*:*:*
policy	cpe:2.3:a:policy:*:*:*:*:*:*:*
postgresql 42.2.14	cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.2.14:*:*:*:*:*:*:*
prettyfaces-jsf2 3.3.0	cpe:2.3:a:apache:prettyfaces-jsf2:3.3.0:*:*:*:*:*:*:*
primefaces 7.0.14	cpe:2.3:a:primetek:primefaces:7.0.14:*:*:*:*:*:*:*

primefaces-extensions 7.0.1	cpe:2.3:a:primetek:primefaces-extensions:7.0.1:*:*:*:*:*:*:*
qname	cpe:2.3:a:qname:*:*:*:*:*:*:*
resolver	cpe:2.3:a:resolver:jar:*:*:*:*:*:*:*
saaj-impl	cpe:2.3:a:sun:saaj:impl:*:*:*:*:*:*:*
sardine	cpe:2.3:a:sardine:*:*:*:*:*:*:*
slf4j-api-1.7.25	cpe:2.3:a:qos:slf4j:1.7.25:*:*:*:*:*:*:*
snmp4j 2.3.4	cpe:2.3:a:snmp4j:2.3.4:*:*:*:*:*:*:*
spring beans 5.2.9	cpe:2.3:a:spring-beans:5.2.9:*:*:*:*:*:*:*
spring context 5.2.9	cpe:2.3:a:spring-context:5.2.9:*:*:*:*:*:*:*
spring core 5.2.9	cpe:2.3:a:spring-core:5.2.9:*:*:*:*:*:*:*
sqljdbc4	cpe:2.3:a:microsoft:sqljdbc4*:*:*:*:*:*:*
sslj	cpe:2.3:a:sslj:*:*:*:*:*:*:*
stax2-api	cpe:2.3:a:stax2-api:*:*:*:*:*:*:*
stax2-api-3.1.4	cpe:2.3:a:stax2-api:3.1.4:*:*:*:*:*:*:*
stax2-api-1.0.2	cpe:2.3:a:stax2-api:1.0.2:*:*:*:*:*:*:*
stax-ex	cpe:2.3:a:stax-ex:*:*:*:*:*:*:*
streambuffer	cpe:2.3:a:streambuffer:*:*:*:*:*:*:*
taglibs-standard 1.2.3	cpe:2.3:a:apache:standard_taglibs:1.2.1:*:*:*:*:*:*:*
tinyradius 1.1.0	cpe:2.3:a:tinyradius:1.1.0:*:*:*:*:*:*:*
tomahawk20-1.1.14	cpe:2.3:a:apache:myfaces_tomahawk:1.1.14:*:*:*:*:*:*:*
unboundid-ldapsdk-4.0.11	cpe:2.3:a:pingidentity:ldapsdk:4.0.11:*:*:*:*:java:*:*
velocity-1.7	cpe:2.3:a:apache:velocity_engine:1.7:*:*:*:*:*:*:*

woodstox-core-asl	cpe:2.3:a:apache:woodstox-core-asl:*:*:*:*:*:*:*
woodstox-core-asl-4.4.1	cpe:2.3:a:apache:woodstox-core-asl:4.4.1:*:*:*:*:*:*:*
wsbuilder	cpe:2.3:a:apache:wsbuilder:*:*:*:*:*:*:*
wsdl4j	cpe:2.3:a:wsdl4j:*:*:*:*:*:*:*
xml-apis 1.3.04	cpe:2.3:a:xmlapis:1.3.04:*:*:*:*:*:*:*
xmlbeans 3.1.0	cpe:2.3:a:apache:xmlbeans:3.1.0:*:*:*:*:*:*:*
xmlgraphics commons 2.2	cpe:2.3:a:apache:xmlgraphics_commons:2.2:*:*:*:*:*:*:*
xmlsec 2.1.4	cpe:2.3:a:xmlseclibs_project:xmlseclibs:2.1.4:*:*:*:*:*:*:*
xmltooling 1.4.6	cpe:2.3:a:xmltooling_project:xmltooling:1.5.4:*:*:*:*:*:*:*
openjdk 1.8.0	cpe:2.3:a:oracle:openjdk:1.8.0:*:*:*:*:*:*:*
microsoft windows server 2016	cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*

The searched components were identified based on processing network traffic and parsing file formats.

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and found that any vulnerabilities have been mitigated or did not result in the TOE being able to be exploited in its evaluated configuration. The search terms, dates, and public databases used are also documented in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP], Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG] and Extended Package for Secure Shell (SSH), Version 1.0, dated 19 February 2016 [SSH-EP] and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

None.

11 Annexes

Not applicable.

12 Security Target

Please see the Fortra's GoAnywhere Managed File Transfer v6.8 Security Target v1.1.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software, version 1.3, dated, 01 March 2019 [SWAPP].
6. Fortra's GoAnywhere Managed File Transfer v6.8 Security Target version 1.1[ST].
7. Fortra's GoAnywhere Managed File Transfer v6.8 Common Criteria Configuration Guide version 1.1[AGD].
8. Evaluation Technical Report for Fortra's GoAnywhere Managed File Transfer v6.8 version 1.1 [ETR].
9. Assurance Activities Report for Fortra's GoAnywhere Managed File Transfer v6.8 version 1.1 [AAR].
10. Fortra's GoAnywhere Managed File Transfer v6.8 Detailed Test Report version 1.4, 3/29/2023. [DTR].