National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Micro Focus Data Protector Premium Edition, 2020.05 (A.10.70)

Report Number: CCEVS-VR-VID11048-2020
Dated: May 26, 2020
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Sheldon Durrant

Randy Heimann

Linda Morrison

Chris Thorpe

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report 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 in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Micro Focus Data Protector Premium Edition release 2020.05, software version A.10.70 (the Target of Evaluation, or 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 as documented in the ST.

The evaluation of the Micro Focus Data Protector Premium Edition release 2020.05, software version A.10.70 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in May 2020.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following document:

- Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The TOE is an enterprise-level software application for Windows that provides backup and restore functionality tailored for enterprise-wide and distributed environments. The focus of the evaluation was on the product’s conformance to the security functionality specified in the following documents:

- Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

The security functions specified in this Protection Profile includes cryptographic modules providing NIST-validated implementations of cryptographic functionality to support secure storage of credentials and secure communications with external IT entities. Data Protector restricts network connections to those required for it to perform its intended functions. Data Protector supports the use of X.509 certificates for authentication of TLS connections. Data Protector is implemented to utilize anti-exploitation capabilities provided by its execution environment. The application installation package and application updates are digitally signed by an authorized source.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the

TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. Therefore, 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.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]

- TD0416: Correction to FCS_RBG_EXT.1 Test Activity
- TD0427: Reliable Time Source
- TD0434: Windows Desktop Applications Test
- TD0437: Supported Configuration Mechanism
- TD0444: IPsec Selections
- TD0445: User Modifiable File Definition
- TD0465: Configuration Storage for .NET Apps
- TD0486: Removal of PP-Module for VPN Clients from allowed with list
- TD0495: FIA_X509_EXT.1.2 Test Clarification
- TD0498: Application Software PP Security Objectives and Requirements Rationale
- TD0505: Clarification of revocation testing under RFC6066

The following NIAP Technical Decisions issued against this PP are not relevant to the TOE:

- TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3—not relevant because the TOE platform is Windows, not Linux
- TD0473: Support for Client or Server TOEs in FCS_HTTPS_EXT—not relevant because the ST does not include HTTPS SFRs.
- TD0510: Obtaining random bytes for iOS/macOS—not relevant because the platform is Windows, not iOS or MacOS.

Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

- TD0442: Updated TLS Ciphersuites for TLS Package
- TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1
- TD0499: Testing with pinned certificates

All other Technical Decisions were found to be not applicable to the TOE, either because they were not related to the claimed Protection Profile or because they related to optional or selection-based functionality that was not claimed in the TOE's Security Target [7].

1.2 Threats

The ST references the PPs to which it claims conformance for statements of threats that the TOE and its operational environment are intended to counter. Those threats, drawn from the claimed PP, are as follows:

- 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.
- 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.
- 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.
- An attacker may try to access sensitive data at rest.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Compliant List (PCL).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Micro Focus Data Protector Premium Edition release 2020.05, software version A.10.70
Sponsor & Developer:	Micro Focus LLC 4555 Great America Parkway Santa Clara, CA 95054
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	May 2020
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	Protection Profile for Application Software, Version: 1.3, 2019-03-01 Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Greg Beaver Kevin Steiner
Validation Personnel:	Sheldon Durrant Randy Heimann Linda Morrison Chris Thorpe

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the ETR.

3.1 Cryptographic Support

The TOE incorporates OpenSSL to provide NIST-validated algorithms for its cryptographic functionality. The TOE provides cryptographic mechanisms for symmetric encryption and decryption, cryptographic signature services, cryptographic hashing services, keyed-hash message authentication services, deterministic random bit generation seeded from a suitable entropy source, key establishment, and secure credential storage. The cryptographic mechanisms support TLS used for secure communication, both as client and server.

3.2 User Data Protection

The TOE leverages the BitLocker functionality of its Windows platform to protect backed-up data written to disk on a Media Agent instance.

Data Protector does not access sensitive information repositories as defined and intended by the Protection Profile for Application Software.

Data Protector restricts network communications to application-initiated network communication for scheduled backup and restore operations.

3.3 Identification and Authentication

The TOE supports the use of X.509 certificates for authentication of TLS connections.

The TOE will not accept a certificate if it is unable to determine the revocation status of the certificate.

3.4 Security Management

The TOE does not create credentials by default. The user logged into the underlying Windows system with admin privileges performs the installation and the TOE subsequently ensures only that user is able to run the TOE.

3.5 Privacy

Data Protector does not collect Personally Identifiable Information (PII) from administrators or users.

3.6 Protection of the TSF

The TOE uses only documented platform APIs.

The TOE does not perform memory mapping to explicit addresses.

The TOE does not make any memory mapping requests with both write and execute permissions.

The TOE runs successfully with process exploit mitigations enabled on the underlying Windows Server platform.

The TOE documentation describes the procedure for users to check for the availability of updates. Data Protector is packaged in the standard Windows Installer (.MSI) format and signed by a code-signing certificate.

The TOE provides the ability to query the current version of the application software.

3.7 Trusted Path/Channels

All data transmitted by Data Protector is assumed to be sensitive data.

A Data Protector instance uses TLS to protect all data it transmits to other Data Protector instances.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- 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.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

4.2 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 evaluation activities specified in Protection Profile for Application Software [6] and Functional Package for Transport Layer Security (TLS) [5] and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Micro Focus Data Protector Security Target, Version 1.0, 6 May 2020 [7].
- The TOE consist of software and leverages the BitLocker functionality of its Windows platform to protect backed-up data written to disk on a Media Agent instance.
- This evaluation did not specifically search for, nor attempt to exploit, 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 TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

The TOE is the Micro Focus Data Protector Premium Edition 2020.05, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report.

The TOE supports a FIPS-mode of operation, which must be enabled in the evaluated configuration to meet the claimed requirements.

The TOE in its evaluated configuration has the following system requirements for its host platforms:

- Data Protector as Cell Manager (including Installation Server and User Interface):
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 16 GB RAM; 5 GB of free disk space + approximately 100 bytes for each backed up file (for use by the IDB)
- Data Protector as Disk Agent:
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 64 MB RAM (128 MB recommended); 20 MB of disk space
- Data Protector as Media Agent:
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 64 MB RAM (128 MB recommended); 20 MB of disk space.

Note: Windows Server 2016 can be running directly on a hardware platform or can be deployed in a VMware ESXi virtual environment. Evaluation testing of the TOE took place on Windows Server 2016 Standard deployed on VMware ESXi 6.5, running on an Intel Xeon Gold 6140 processor (Skylake microarchitecture).

The following network port must be open for the TOE to function:

- 5565 – port required for new installation in Data Protector.

If the TOE is installed in a virtual environment, then it must be the only guest running in the virtualized environment.

5.2 Excluded Functionality

The backup and restore functions provided by Data Protector Premium Edition, release 2020.05, software version A.10.70 are not covered by any security functional requirements and so were not addressed by the evaluation. The evaluation covered the ability of the TOE to protect data transmitted between separate TOE instances using TLS, but did not cover the actual backup and restore functions of the TOE.

- Remote administration—in the evaluated configuration, the User Interface component must be installed only on the same platform as the TOE instance in the Cell Manager role, thus providing local administration for the Cell Manager. The User Interface is not to be installed on other platforms in the network (e.g., administrator workstations) and remote administration is not supported.
- Remote authentication—the product supports remote authentication using LDAP, but this capability was not tested, nor was the ability of the product to protect communications with the external LDAP server using TLS.

- REST API—the product provides a REST API to access management functionality, but this interface is excluded from use in the evaluated configuration.

6 Documentation

Micro Focus offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- Data Protector, Version: 2020.05 [8]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in this guide.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- Micro Focus Data Protector Premium Edition 2020.05 (A.10.70) Common Criteria Test Report and Procedures For Application Software PP Version 1.3 [9]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report For Micro Focus Data Protector Premium Edition 2020.05 (A.10.70) [10]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the Functional Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. Testing of the TOE was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from March 1, 2020 to April 14, 2020.

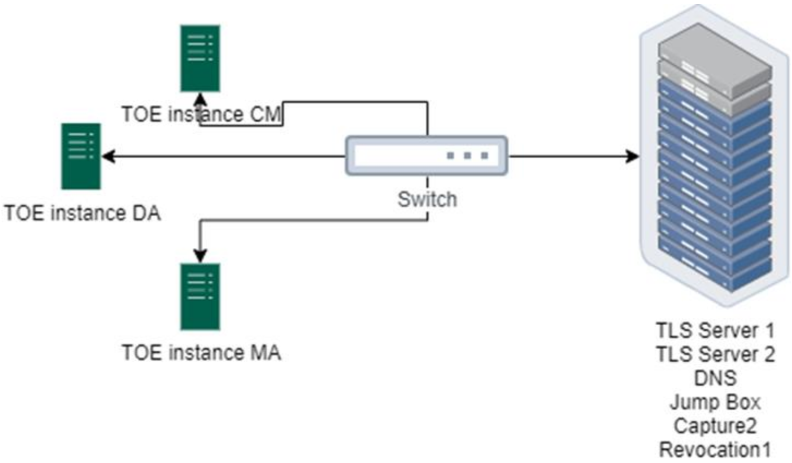
Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6] were fulfilled.

7.1 Test Configuration

The test environment included the following elements:

- TOE instance Cell Manager (CM)
    - Windows Server 2016 Standard on ESXi 6.5
    - Micro Focus Data Protector 2020.05 (A.10.70) Cell Manager role
- TOE instance Disk Agent (DA)
    - Windows Server 2016 Standard on ESXi 6.5
    - Micro Focus Data Protector 2020.05 (A.10.70) Disk Agent role
- TOE instance Media Agent (MA)
    - Windows Server 2016 Standard on ESXi 6.5
    - Micro Focus Data Protector 2020.05 (A.10.70) Media Agent role
- Jump Box
    - xca 2.1.2 for PKI management
- TLS test server 1—used to test TLSC, TLSS, and X509 requirements
    - Ubuntu 18.04
    - OpenSSL 1.1.1
    - Custom Lab TLS Server and Client test tools

- TLS test server 2—used to test TLSC, TLSS, and X509 requirements
    - Ubuntu 18.04
    - Custom Lab TLS Server and Client test tools
- Capture2—used for packet capture
    - Windows Server 2012 R2
    - Wireshark 3.2.0
- DNS—function as a DNS server
    - Windows Server 2016
- Revocation1—function as an OCSP responder
    - Ubuntu 18.04



The TOE must be deployed as described in section **Error! Reference source not found.**.1 of this Validation Report and be configured in accordance with the *Data Protector, Version: 2020.05* [8] administrative guide.

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles. This included a search of public vulnerability databases and running a virus scanner with the most current virus definitions against the application files in accordance with Section 5.2.6 of [6].

The evaluation team searched the following data bases:

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- https://cve.mitre.org/cve/search_cve_list.html
- https://www.openssl.org/news/vulnerabilities

Searches were performed on 4/17/2020.

The keyword searches included the following terms:

- Search Terms:
- Micro Focus

- Data Protector
- OpenSSL 1.0.2u
- Windows Server 2016
- CVE-2020-0601
- TCP
- TLS
- Backup, Vendor = microfocus

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Protection Profile for Application Software, Version 1.3, 1 March 2019* [6]
- *Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019* [5]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	ALC_TSU_EXT.1 Timely Security Updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Data Protector Guidance Document, Version: 2020.05. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness for this evaluation.

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *Micro Focus Data Protector Security Target, Version 1.0, 6 May 2020* [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

[5] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019

[6] Protection Profile for Application Software, Version: 1.3, 2019-03-01

[7] Micro Focus Data Protector Security Target, Version 1.0, 6 May 2020

[8] Data Protector, Version: 2020.05

[9] Micro Focus Data Protector Premium Edition 2020.05 (A10.70) Common Criteria Test Report and Procedures For Application Software PP, Version 1.3, 7 May 2020

[10] Assurance Activities Report For Micro Focus Data Protector Premium Edition, 2020.05 (A.10.70) Version 1.0, 7 May 2020