Certificate Report

Version 1.0

20 April 2023

CSA_CC_21001

For

Belden Hirschmann IT MTS Series Ethernet Switches v9.7.202.3 (for box switch) v9.7.202.3 (for chassis switch)

From

Belden Hirschmann Industries (Suzhou) Ltd

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	20 April 2023	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Belden Hirschmann IT MTS Series Ethernet Switches, v9.7.202.3 (for box switch) v9.7.202.3 (for chassis switch), and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Belden Hirschmann IT MTS Series Ethernet Switches (Box Switch/Chassis Switch)	V9.7.202.33
Firmware	V9.7.202.33

Table 1 - TOE components identifier

The TOE comes in 2 different physical platforms: Box switch and Chassis switch. Both platform series of switches are Layer 3 switches, operates on the same firmware, provides the same security functionalities, and supports the Open Shortest Path First (OSPF) protocol.

Capacity wise, the Chassis Switch has a larger forwarding capacity and also uses a different Line Processing Unit (LPU) to provide different port options.

Model	Platform
MTS2724-4X-FP-	Box Switch
MTS2848-6X-E	
MTS2824-6X-E	
MTS2848-6X-S	
MTS2824-4X-S	
MTS2824F-4X-S	
MTS2832TF-4X-E	
MTS2748-6X-MP-E	
MTS2724-6X-MP-E	
MTS2948X-6Q-A	
MTS8003	Chassis Switch
MTS8006	
MTS8010	

Table 2 - TOE Platform Identifiers

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version	Method of Delivery
Safety and general information guide	1.0	Packaged with the switch and delivered by courier service
Operational installation user guidance	1.0	Belden Website
User Manual	1.3	Belden Website

Table 3 - List of guidance documents

The evaluation of the TOE has been carried out by An Security, an approved CC test laboratory, at the assurance level CC EAL 2 augmented with ALC_FLR.2 and completed on 19 April 2023.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
Authentication
Traffic Forwarding
Auditing
Communications Security
IP-based ACL
Cryptographic Function
Security Functionality Management
Access Control

Table 4: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.