Certification Report

Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3

Sponsor and developer: ***Cisco Systems, Inc.***
170 West Tasman Dr.
San Jose, CA 95134
USA

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-14-39582-CR**

Report version: **1**

Project number: **NSCIB-CC-14-39582**

Authors(s): **Denise Cater**

Date: **November 27, 2014**

Number of pages: **14**

Number of appendices: **0**

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**C14-39582**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Cisco Systems, Inc.** **170 West Tasman Dr., San Jose, CA 95134, USA**
Product and assurance level	**Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3,** Assurance Package: ▪ EAL3
Project number	**NSCIB-CC-14-39582-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **27-11-2014**

Certificate expiry : **27-11-2019**

Registration number

PRODUCTS
RvA C 078

Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 (hereinafter referred to as Cat3K6K). The developer of the Cat3K6K is Cisco Systems, Inc located in San Jose, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a switching and routing platform used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer2 switch, it performs analysis of incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. As a Layer3 switch/router, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet. Routing protocols used by the TOE include BGPv4, EIGRP, EIGRPv6 for IPv6 and OSPFv2. BGPv4, EIGRP and EIGRPv6 supports routing updates with IPv6 or IPv4, while OSPFv2 routing protocol support routing updates for IPv4 only.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 26 November 2014 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Cat3K6K, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Cat3K6K are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL3 assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 from Cisco Systems, Inc located in San Jose, USA.

The TOE is comprised of the following main components:

3850 Switch Delivery item type	Identifier	Version
Hardware	Cisco Catalyst 3850 (WS-C3850-24T, WS-C3850-48T, WS-C3850-24P, WS-C3850-48P, WS-C3850-48F, WS-C3850-24U, WS-C3850-48U, WS-C3850-12S, WS-C3850-24S) with Network Modules (C3850-NM-4-1G, C3850-NM-2-10G and C3850-NM-4-10G)	N/A
Software	IOS-XE	3.6.0E

6500 Switch Delivery item type	Identifier	Version
Hardware	Cisco Catalyst 6500 (WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, WS-C6513-E), with one or two Supervisor 2T (Sup 2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) and one or more Line Cards (note, line cards are not TSF enforcing): 40G Ethernet Interfaces, including WS-X6904-40G-2T (with DFC4) and WS-X6904-40G-2TXL (with DFC4XL)/10G Ethernet Interfaces, including WS-X6908-10G-2T (with DFC4), WS-X6908-10G-2TXL (with DFC4XL), WS-X6816-10T-2T (with DFC4), WS-X6816-10T-2TXL (with DFC4XL), WS-X6816-10G-2T (with DFC4), WS-X6816-10G-2TXL (with DFC4XL), WS-X6716-10T-3C, WS-X6716-10T-3CXL, WS-X6704-10GE, WS-X6708-10G-3C, WS-X6708-10G-3CXL, WS-X6716-10GT-3C, WS-X6716-10GT-3CXL/Gigabit Ethernet Interfaces, including WS-X6824-SFP-2T (with DFC4), WS-X6824-SFP-2TXL (with DFC4XL), WS-X6848-SFP-2T (with DFC4), WS-X6848-SFP-2TXL (with DFC4XL), WS-X6848-TX-2T (with DFC4), WS-X6848-TX-2TXL (with DFC4XL), WS-X6748-SFP, WS-X6724-SFP, WS-X6516A-GBIC, WS-X6408A-GBIC	N/A
Software	IOS	15.1(2)SY3

To ensure secure usage a set of guidance documents is provided together with the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TOE are:

- Ø The TOE generates audit messages that identify specific TOE operations;

- The TOE provides cryptography support for secure communications and protection of information;
- VLANs control whether Ethernet frames are passed through the switch interfaces based on the VLAN tag information in the frame header;
- IP ACLs control whether routed IP packets are forwarded or blocked at Layer 3 TOE interfaces (interfaces that have been configured with IP addresses);
- VACLs (using access mapping) control whether non-routed frames (by inspection of MAC addresses in the frame header) and packets (by inspection of IP addresses in the packet header) are forwarded or blocked at Layer 2 ports assigned to VLANs;
- The TOE performs authentication, using Cisco IOS/IOS-XE platform authentication mechanisms, to authenticate user access. The TOE supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users;
- The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE;
- The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and access controls to limit configuration to authorized administrators;
- The TOE can terminate inactive sessions after an authorized administrator configurable time-period and can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

Detailed information on the assumptions and threats can be found in the *[ST]* sections 3.3 and 3.4 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

- Administrators will periodically review the audit logs to identify sources of concern;
- Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators.

2.3.2 Environmental assumptions

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definition of the assumption refer to the *[ST]*, chapter 3.3):

- Administrators are assumed to be non-malicious with appropriate training.
- The TOE will be physically protected within controlled access facilities;
- The TOE is interoperable with other Cisco products and the software and hardware of other switch vendors on the network;
- The threat of malicious attacks aimed at exploiting the TOE is considered low.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 3.5):

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

2.4 Architectural Information

The general architecture consists of the following functionalities:

1. The *Runtime functionality* which provides core OS functionality (including system clock). It provides the hardware interfaces used by the TSFI
2. The *Crypto Engine* functionality that implements support for cryptographic operations used by other parts of the TOE
3. The *SSH functionality* that provides SSHv2 server capability that allows administrators to establish a secured (encrypted) communication pathway between their SSH client and the TOE. This pathway is use to provide the CLI interface to the administrator for use in managing and configuring the TOE.
4. The *Firewall functionality* that processes network traffic and permit or deny traffic flows. Includes all protocol support required for the TOE to accept network traffic from either Internal Network or External network and enforce the configured security policy.
5. The *CLI functionality* that accepts administrative input from an external terminal. The CLI is a basic Command Line Interface. Other management interfaces exist (e.g. http(s)-based, snmp-based) but these are not allowed in the evaluated configuration, as per the Guidance.
6. The *Logging Functionality* that receives system event messages from other functionalities and sends them to (configurable):
   - The console
   - An internal buffer for storage
   - An external syslog server
7. The *AAA functionality* that provides authentication: RADIUS, TACACS+ or local authentication

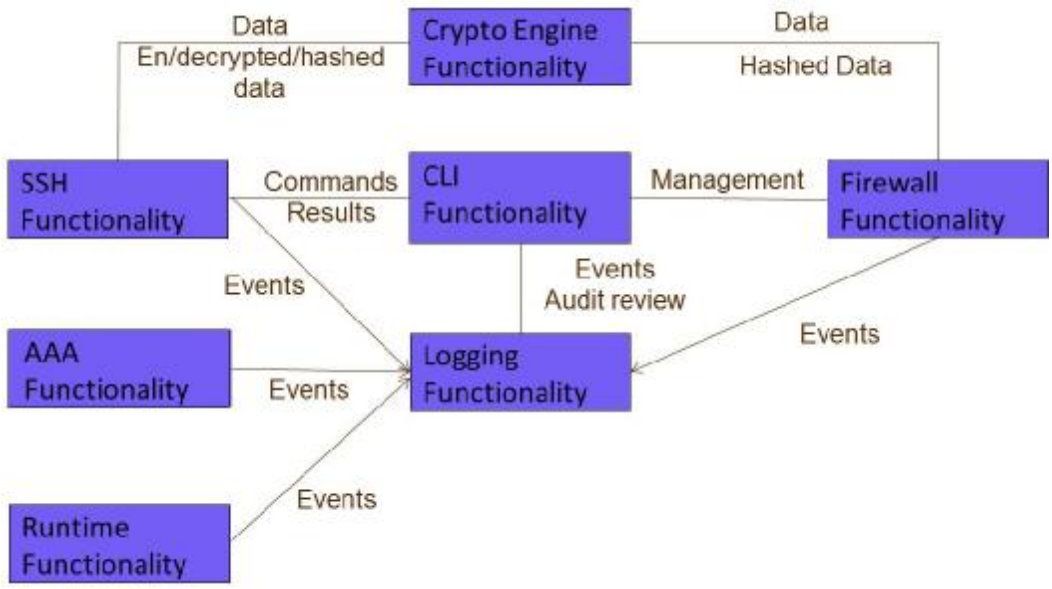

Figure 1 TOE Architecture

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 Common Criteria Operational User Guidance and Preparative Procedures	V1.0, 15-10-2014

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): Brightsight executed the developer tests as consultancy. For this reason, Brightsight did not repeat these developer tests as no additional product assurance would be gained through this activity.

2.6.1 Testing approach and depth

The developer tests consist of 25 tests, some of which were quite extensive. These tests cover all TSFI and all SFRs and include both positive and negative tests.

In additional to the developer tests, the evaluator has derived and executed 7 additional functional tests.

2.6.2 Independent Penetration Testing

The evaluators performed 29 penetration tests. These were derived from a vulnerability analysis comprised of 3 parts:

1. Public domain vulnerability analysis of TOE specific vulnerabilities (vulnerabilities specific for 3850/6500 series hardware and IOS-XE 3.6.0E / IOS 15.1.(1)SY3 software);
2. Public domain vulnerability analysis of TOE-type vulnerabilities (vulnerabilities that are generic for routers/switches);
3. Analysis of TOE deliverables (FSP/TDS etc.).

2.6.3 Test Configuration

The network diagram in Figure 2 describes the overall setup of the lab and the IP addresses used for developer and evaluator testing. Ports are labelled as follows:

- Ø Ports on the router (TOE) are labelled with R (RA, RB, RC for regular interfaces, RL for loopback interface, RM for management interface);
- Ø Ports on the Testing computer are labelled T (TA, TB, TC for regular interfaces, TL for loopback interface);
- Ø SER is the serial port on the testing computer and CO is the console port of the TOE.

As the evaluator executed the same tests on multiple platforms (in this case, 6500 series and 3850 series Cisco switches) testing was performed using primarily python scripts running on the testing computer. The configurations of RADIUS, TACACS+, NTP, and Syslog services were fixed throughout the process.

The following evaluation tools were used for testing:

Description	Package Name	Platform	Version
Linux Kernel	linux-image-3.2.0-4-486	i386	3.2.57-3
SSH Client Software	openssh-client	i386	1:6.0p1-4+deb7ul
RADIUS Server	freeradius	i386	2.1.12+dfsg-1.2
TACACS+ Server	tacacs+	i386	4.0.4.19-11
NTP Server	ntp	i386	1:4.2.6.p5+dfsg-2
Syslog Server	rsyslog	i386	5.8.11-3
OSPF/BGP Implementation	quagga	i386	0.99.22.4-1+wheezy1
Test Automation	python-pexpect	i386	2.4-1
Test Automation	python-scapy	i386	2.2.0-1

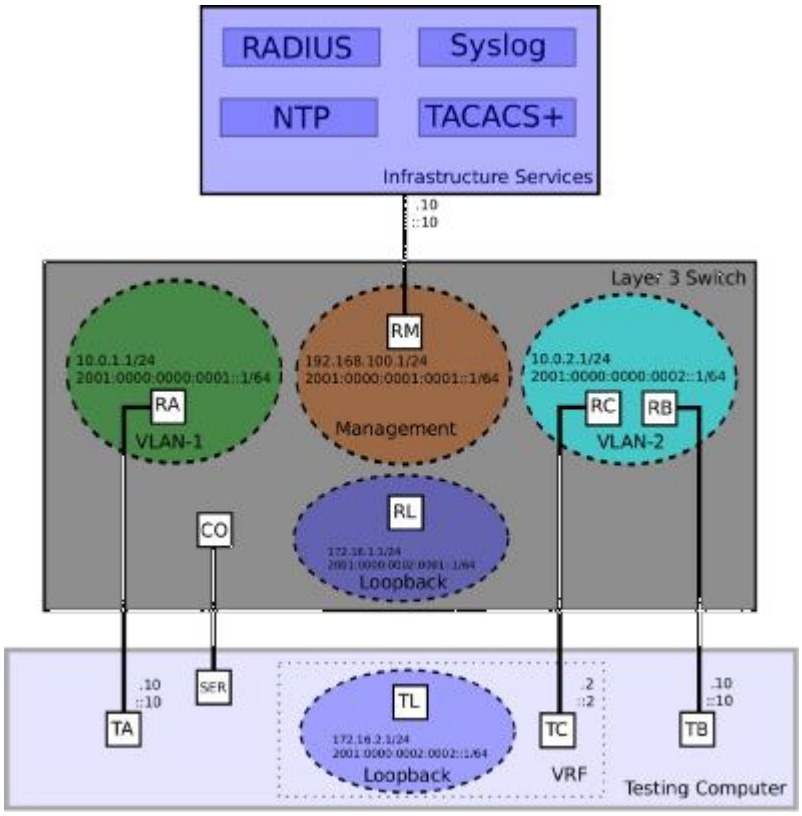

Figure 2 Test Configuration

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents. The verdict of each claimed assurance requirement is "Pass".

Based on the evaluation results the evaluation lab concluded the Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3**. This implies that the product satisfies the security technical requirements specified in Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 Security Target.

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

The customer must/shall follow the provided guidance documentation in *[AGD]*, in particular:

- It is the customer's responsibility to configure secure connection between the TOE and the NTP Server / Authentication Server / Syslog Server.
- Although the TOE supports additional algorithms and protocols, the customer should be aware that only those specified in *[ST]* and *[AGD]* are supported in the evaluated configuration.

3 Security Target

The Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 Security Target *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AAA	Authentication, Authorization & Accounting
ACL	Access Control List
BGP	Border Gateway Protocol
CLI	Command Line Interface
EIGRP	Enhanced Interior Gateway Routing Protocol
HTTPs	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
OSPF	Open Shortest Path First
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TOE	Target of Evaluation
VACL	VLAN ACL
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[AGD]	Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 Common Criteria Operational User Guidance and Preparative Procedures, v1.0, 15 October 2014
[CC]	Common Criteria for Information Technology Security Evaluation, Part I, Part II and III, version 3.1, revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.
[ETR]	Brightsight, Evaluation Technical Report Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2) v1.0 EAL3, 14-RPT-302, version 1.2, 25 November 2014.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 2.1, 1 August 2011.
[NSP#6]	NSCIB Scheme Procedure #6, Alternative Evaluator Reporting, Version 1.2, May 20, 2014
[ST]	Cisco Catalyst 3850 Series Switches running IOS-XE 3.6.0E and Catalyst 6500 Series Switches running IOS 15.1(2)SY3 Security Target, revision 1.0, 15 October 2014.

(This is the end of this report).