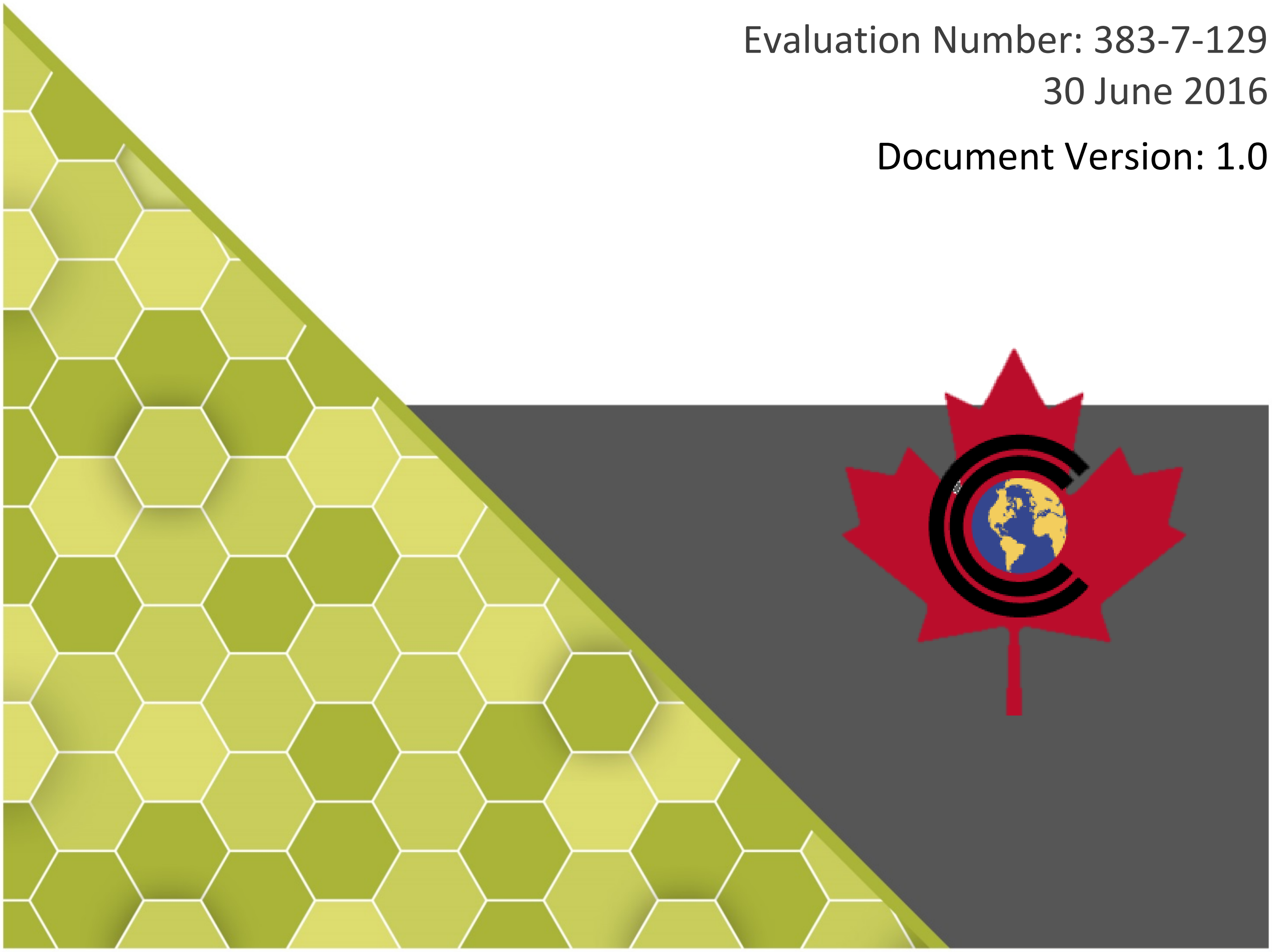
Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA MAINTENANCE REPORT

API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0

Evaluation Number: 383-7-129
30 June 2016

Document Version: 1.0



Canada

FOREWORD

This maintenance report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

If your department has identified a requirement for report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

EWA-Canada has submitted the Impact Analysis Report (IAR) for API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0 (hereafter referred to the TOE), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

TABLE OF CONTENTS

1 Changes ... 1

1.1 Description of changes in the Maintained Target of Evaluation ... 1

1.2 Description of Changes to the IT Environment ... 2

1.3 Affected developer evidence ... 2

2 Conclusions ... 3

2.1 References ... 3

1 CHANGES

The following characterizes the changes implemented in the TOE and the environment. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained.

1.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise;

- Feature enhancements that do not affect the existing security features of the of TOE;
- Resolution of POODLE vulnerability;
- Resolution of Shellshock vulnerability;
- Routing Device request time out error when connecting to APL 2 endpoints fixed;
- ALARMDISPATCH script now handles SYSTEM_ALARMs correctly;
- PRIISMS used to orphan APL2 connections;
- The IPSECSTARTUP script no longer runs every time PRIISMS starts;
- Uninstall problems with PRIISMS 2.8 were fixed;
- Setup of PRIISMS 2.8 now finishes properly;
- For CreateAPL2Connection Script - Client IP Pool Start Address hardcoded to 1.254.254.254 no longer reduces to 1.254.254.1;
- AGM Module now validates Type (RADIUS or TACACS), which used to cause PRSERVER to crash;
- ALARMDISPATCH Script now runs only once at the same time so that there are not multiple emails for the same alarm;
- PRIISMS now does not allow the same serial number to be used for multiple site records;
- PRIISMS now causes tunnel to disconnect when Site Record is deleted or SSL/VPN Checkbox is unchecked;
- Bug fixed of APL2EndpointAddressPoolList changes not sent to PRIISMS Routing Device immediately, but PRIISMS used the new list as though it had;
- RADIUS did not work with PRIISMS;
- Can now access endpoints after PRIISMS is rebooted;
- '+' now an acceptable character in the endpoint ID for APL2;
- My Conns TAB used to display only APL2 connections;
- PRIISMS used to treat generic APL2 ports the same as SnapNAT ports even though they are different;

- Bugs fixed in AGM module;
- SnapNAT NOC Tools had access to all APL2 defined ports;
- No longer possible to add an empty record for SnapNAT endpoint;
- Creation of Host type endpoint now defines correct IP port number;
- Version number of the file now written to the monitor log file for PRIISMS executables; and
- PRIISMS now cycles tunnel when Site Details are changed.

1.2 DESCRIPTION OF CHANGES TO THE IT ENVIRONMENT

The changes to the IT environment comprise;

- PRIISMS 3.0 now supports installations on Windows Server 2012 R2 using SQL Server 2012.

1.3 AFFECTED DEVELOPER EVIDENCE

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

2 CONCLUSIONS

Through functional and regression testing of the TOE, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme 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. These evaluation results apply 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 Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

2.1 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011.
Certification Report API Technologies IOS SA5600 v1.3.1 with PRIISMS v2.8.1, v1.0, 2 July 2014
Security Target API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0, v1.19, 14 June 2016