



COMMON CRITERIA MAINTENANCE REPORT

VMware NSX v6.3.1 for vSphere

383-7-149

December 06, 2017

1.0





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

CGI IT Security Evaluation & Test Facility has submitted the Impact Analysis Report (IAR) for VMware NSX v6.3.1 for vSphere (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	5
1.1	Description of changes in the Maintained Target of Evaluation	5
1.2	Affected developer evidence.....	5
2	Conclusions	6
2.1	References	6



1 CHANGES

The following characterizes the changes implemented in the TOE and/or 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;

- Various bug fixes and feature enhancements resulting from defects detected and resolved through the QA/test process that do not affect the existing security features of the of TOE;
- Addition of CrossVC functionality (not included within the scope of the evaluation);
- Update JRE to 1.7 / 101 to address the following CVEs;
 - CVE-2016-3500
 - CVE-2016-3508
 - CVE-2016-3485
- Fix to address Dirty Cow Linux Kernel Vulnerability, CVE-2016-5195; and
- Hardening of the TOE in the event of a component failure.

1.2 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 previously 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.

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 Instruction #5, Assurance Continuity Requirements, v1.0, May 2017.
Certification Report for VMware NSX v6.3 for vSphere, 30 March 2017, v1.0
Security Target VMware NSX 6.3.1 for vSphere, 29 November 2017, v2.6