Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

COMMON CRITERIA MAINTENANCE REPORT

Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978.444.444, Solutions Enabler 9.1 and Unisphere for PowerMax 9.1 with security patches: DSA-2019-186, DSA-2019-193, DSA-2020-062, DSA-2020-065, DSA-2020-130, DSA-2020-221

15 March 202

447-EWA-MR

Canada

FOREWORD

This Maintenance Report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The IT product identified in this report has been previously evaluated at an approved Common Criteria testing lab established under the Canadian Common Criteria program using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5.

This report is not an endorsement of the IT product by the Canadian Centre for Cyber Security, and no warranty of the IT product by the Canadian Centre for Cyber Security is expressed or implied.

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

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

TABLE OF CONTENTS

1 INTRODUCTION

An Impact Analysis Report was submitted to the Canadian Common Criteria program to extend the validity of the Common Criteria certificate previously awarded to **Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978.144.144, Solutions Enabler 9.0 and Unisphere for PowerMax 9.0.0.6**.

The process to achieve this under mutual recognition is described in Assurance Continuity: CCRA Requirements, version 2.1, June 2012. In accordance with the requirements of this process, the Impact Analysis Report describes all changes made to the product and/or its IT environment, all resulting changes made to the evaluation evidence, and the security impact of the changes.

The purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978.444.444, Solutions Enabler 9.1 and Unisphere for PowerMax 9.1 with security patches: DSA-2019-186, DSA-2019-193, DSA-2020-062, DSA-2020-065, DSA-2020-130, DSA-2020-221**, hereafter referred to as the maintained Target of Evaluation, or maintained TOE.

2 DESCRIPTION OF CHANGES

The following characterizes the changes implemented in the maintained TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the Security Target.

2.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the maintained TOE comprise the following:

- Bug fixes resulting from defects detected and resolved through the Quality Assurance/test process,
- Feature enhancements that do not affect the established security baseline,
- Patches for the following CVEs:

CVE-2019-2949 CVE-2019-2989 CVE-2019- 2958 CVE-2019-2977 CVE-2019-2975 CVE-2019-2999

CVE-2019-2996 CVE-2019-2987 CVE-2019-2962 CVE-2019-2988 CVE-2019-2992 CVE-2019-2964

CVE-2019-2973 CVE-2019-2981 CVE-2019-2978 CVE-2019-2894 CVE-2019-2983 CVE-2019-2933

CVE-2019-2945 CVE-2019-11068 CVE-2019-0887 CVE-2019-1006 CVE-2019-1071 CVE-2019-1073

CVE-2019-1082 CVE-2019-1085 CVE-2019-1088 CVE-2019-1089 CVE-2019-1093 CVE-2019-1094

CVE-2019-1095 CVE-2019-1096 CVE-2019-1097 CVE-2019-1098 CVE-20191099 CVE-2019-1100

CVE-2019-1101 CVE-2019-1102 CVE-2019-1108 CVE-2019-1116 CVE-2019-1132 CVE-2019-0683

CVE-2019-0888 CVE-2019-0904 CVE-2019-0905 CVE-2019-0906 CVE-2019-0907 CVE-2019-0908

CVE-2019-0909 CVE-2019-0941 CVE-2019-0943 CVE-2019-0948 CVE-2019-0960 CVE-2019-0968

CVE-2019-0972 CVE-2019-0973 CVE-2019-0974 CVE-2019-0977 CVE-2019-0984 CVE-2019-0985

CVE-2019-0986 CVE-2019-1009 CVE-2019-1010 CVE-2019-1011 CVE-2019-1012 CVE-2019-1013

CVE-2019-1014 CVE-2019-1015 CVE-2019-1016 CVE-2019-1017 CVE-2019-1019 CVE-2019-1025

CVE-2019-1028 CVE-2019-1039 CVE-2019-1040 CVE-2019-1043 CVE-2019-1045 CVE-2019-1046

CVE-2019-1047 CVE-2019-1048 CVE-2019-1049 CVE-2019-1053 CVE-2017-8533 CVE-2019-0708

CVE-2019-0734 CVE-2019-0758 CVE-2019-0863 CVE-2019-0881 CVE-2019-0882 CVE-2019-0885

CVE-2019-0889 CVE-2019-0890 CVE-2019-0891 CVE-2019-0893 CVE-2019-0894 CVE-2019-0895

CVE-2019-0896 CVE-2019-0897 CVE-2019-0898 CVE-2019-0899 CVE-2019-0900 CVE-2019-0901

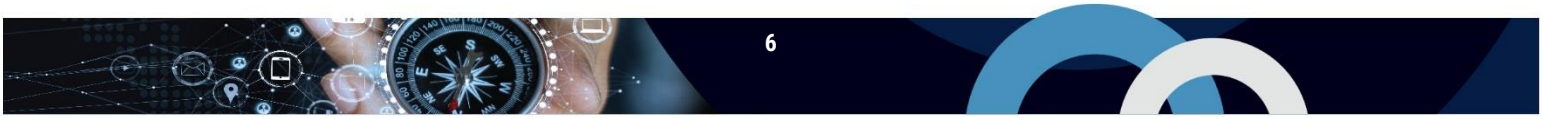
CVE-2019-0902 CVE-2019-0903 CVE-2019-0936 CVE-2019-0961 CVE-2019-1001 CVE-2019-1004

CVE-2019-1056 CVE-2019-1059 CVE-2019-1063 CVE-2019-1104 CVE-2019-18588 CVE-2020-2604

CVE-2020-2601 CVE-2020-2585 CVE-2020-2655 CVE-2020-2593 CVE-2020-2654 CVE-2020-2590

CVE-2020-2659 CVE-2020-2583 CVE-2019-16168 CVE-2019-13117 CVE-2019-13118 CVE-2019-1552

CVE-2019-1563 CVE-2019-1551 CVE-2019-1547 CVE-2019-1559 CVE-2019-12572 CVE-2018-0734
CVE-2018-0732 CVE-2017-3737 CVE-2017-3731 CVE-2017-3738 CVE-2017-3732 CVE-2016-8610
CVE-2016-2107 CVE-2016-0702 CVE-2016-0797 CVE-2016-0799 CVE-2016-2842 CVE-2016-0703
CVE-2016-0704 CVE-2016-0800 CVE-2016-6304 CVE-2016-6306 CVE-2016-2105 CVE-2016-2106
CVE-2016-0701 CVE-2016-2109 CVE-2015-1794 CVE-2015-1787 CVE-2015-3197 CVE-2015-3194
CVE-2015-3195 CVE-2015-3196 CVE-2015-1792 CVE-2015-0207 CVE-2015-0208 CVE-2015-0285
CVE-2015-0288 CVE-2015-0290 CVE-2015-0291 CVE-2015-0293 CVE-2015-3193 CVE-2015-1788
CVE-2015-1789 CVE-2015-1790 CVE-2015-1791 CVE-2015-0209 CVE-2015-0286 CVE-2015-0287
CVE-2015-0289 CVE-2013-6449 CVE-2020-0607 CVE-2020-0615 CVE-2020-0608 CVE-2020-0611
CVE-2020-0620 CVE-2020-0625 CVE-2020-0626 CVE-2020-0627 CVE-2020-0628 CVE-2020-0629
CVE-2020-0630 CVE-2020-0632 CVE-2020-0631 CVE-2020-0634 CVE-2020-0635 CVE-2020-0639
CVE-2020-0643 CVE-2020-0642 CVE-2020-0640 CVE-2020-0673 CVE-2020-0674 CVE-2019-1458
CVE-2019-1469 CVE-2019-1474 CVE-2019-1478 CVE-2019-1488 CVE-2019-1453 CVE-2019-1465
CVE-2019-1466 CVE-2019-1467 CVE-2019-1468 CVE-2019-1481 CVE-2019-1480 CVE-2019-1484
CVE-2019-1485 CVE-2019-1384 CVE-2019-1388 CVE-2019-1391 CVE-2019-1393 CVE-2019-1394
CVE-2019-1395 CVE-2019-1407 CVE-2019-1411 CVE-2019-1409 CVE-2019-1415 CVE-2019-1418
CVE-2019-1419 CVE-2019-1424 CVE-2019-1432 CVE-2019-1433 CVE-2019-1434 CVE-2019-1435
CVE-2019-1438 CVE-2019-1441 CVE-2019-1439 CVE-2019-1456 CVE-2019-1382 CVE-2019-1396
CVE-2019-1405 CVE-2019-1408 CVE-2019-1412 CVE-2019-1406 CVE-2019-1422 CVE-2019-1429
CVE-2019-1390 CVE-2019-11135 CVE-2020-5367 CVE-2020-5345 CVE-2020-2805 CVE-2019-18197
CVE-2020-2816 CVE-2020-2781 CVE-2020-2830 CVE-2020-2767 CVE-2020-2800 CVE-2020-2778
CVE-2020-2764 CVE-2020-2754 CVE-2020-2755 CVE-2020-2773 CVE-2020-2756 CVE-2020-2757
CVE-2020-0821 CVE-2020-0907 CVE-2020-0988 CVE-2020-0987 CVE-2020-0992 CVE-2020-0993
CVE-2020-0999 CVE-2020-1004 CVE-2020-1005 CVE-2020-1007 CVE-2020-1008 CVE-2020-1014
CVE-2020-1015 CVE-2020-1094 CVE-2020-0687 CVE-2020-0889 CVE-2020-0938 CVE-2020-0946
CVE-2020-0952 CVE-2020-0953 CVE-2020-0955 CVE-2020-0957 CVE-2020-0956 CVE-2020-0958
CVE-2020-0959 CVE-2020-0960 CVE-2020-0962 CVE-2020-0964 CVE-2020-0965 CVE-2020-0994
CVE-2020-0982 CVE-2020-0995 CVE-2020-1000 CVE-2020-1009 CVE-2020-1011 CVE-2020-1020
CVE-2020-1027 CVE-2020-0684 CVE-2020-0772 CVE-2020-0774 CVE-2020-0791 CVE-2020-0804
CVE-2020-0842 CVE-2020-0843 CVE-2020-0844 CVE-2020-0845 CVE-2020-0849 CVE-2020-0871



CVE-2020-0645 CVE-2020-0769 CVE-2020-0770 CVE-2020-0771 CVE-2020-0773 CVE-2020-0779 CVE-2020-0778 CVE-2020-0781 CVE-2020-0783 CVE-2020-0785 CVE-2020-0787 CVE-2020-0788 CVE-2020-0802 CVE-2020-0803 CVE-2020-0806 CVE-2020-0814 CVE-2020-0822 CVE-2020-0853 CVE-2020-0860 CVE-2020-0877 CVE-2020-0879 CVE-2020-0880 CVE-2020-0881 CVE-2020-0883 CVE-2020-0882 CVE-2020-0885 CVE-2020-0887 CVE-2020-0655 CVE-2020-0657 CVE-2020-0665 CVE-2020-0666 CVE-2020-0668 CVE-2020-0667 CVE-2020-0675 CVE-2020-0676 CVE-2020-0677 CVE-2020-0678 CVE-2020-0681 CVE-2020-0680 CVE-2020-0682 CVE-2020-0683 CVE-2020-0686 CVE-2020-0698 CVE-2020-0703 CVE-2020-0726 CVE-2020-0658 CVE-2020-0691 CVE-2020-0705 CVE-2020-0708 CVE-2020-0715 CVE-2020-0719 CVE-2020-0720 CVE-2020-0721 CVE-2020-0722 CVE-2020-0723 CVE-2020-0725 CVE-2020-0724 CVE-2020-0729 CVE-2020-0734 CVE-2020-0730 CVE-2020-0731 CVE-2020-0736 CVE-2020-0735 CVE-2020-0738 CVE-2020-0737 CVE-2020-0744 CVE-2020-0748 CVE-2020-0745 CVE-2020-0753 CVE-2020-0752 CVE-2020-0754 CVE-2020-0755 CVE-2020-0756 CVE-2020-0895 CVE-2020-0967 CVE-2020-0966 CVE-2020-0968 CVE-2020-0768 CVE-2020-0847 CVE-2020-0824 CVE-2020-0830 CVE-2020-0832 CVE-2020-0833 CVE-2020-0673 CVE-2020-0674 CVE-2020-0606 CVE-2020-0646 CVE-2020-0605 CVE-2020-14664 CVE-2020-14583 CVE-2020-14593 CVE-2020-14562 CVE-2020-14621 CVE-2020-14556 CVE-2020-14573 CVE-2020-14581 CVE-2020-14578 CVE-2020-14579 CVE-2020-14577 CVE-2019-8331.

2.2 AFFECTED DEVELOPER EVIDENCE

Modifications to the product necessitated changes to the following developer evidence that was previously submitted in support of the original evaluation:

The following developer evidence changes have occurred:

- ST updates:
  - Title page
  - ST Reference (section 1.2)
  - TOE Reference (section 1.3)
  - Table 1 – TOE Hardware and Software

NOTE: User guides – original guidance can be applied to the TOE. No change

3 CONCLUSIONS

Through functional and regression testing of the maintained TOE, assurance gained in the original TOE certification was maintained. As all 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 maintenance and re-evaluation is not required.

4 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS 5978, 15 October 2018, 383-4- 447, V1.0
Security Target Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS5978.444.444, Solutions Enabler 9.1 and Unisphere for PowerMax 9.1 with security patches: DSA-2019-186, DSA-2019-193, DSA-2020-062, DSA-2020-065, DSA-2020-130, DSA-2020-221, 15 March 2021, v1.6
Impact Analysis Report Dell EMC™ VMAX® All Flash and PowerMax™ with PowerMaxOS5978.444.444, Solutions Enabler 9.1 and Unisphere for PowerMax 9.1 with security patches: DSA-2019-186, DSA-2019-193, DSA-2020-062, DSA-2020-065, DSA-2020-130, DSA-2020-221, 15 March 2021, v1.6.