Communications Security Establishment   Centre de la sécurité des télécommunications

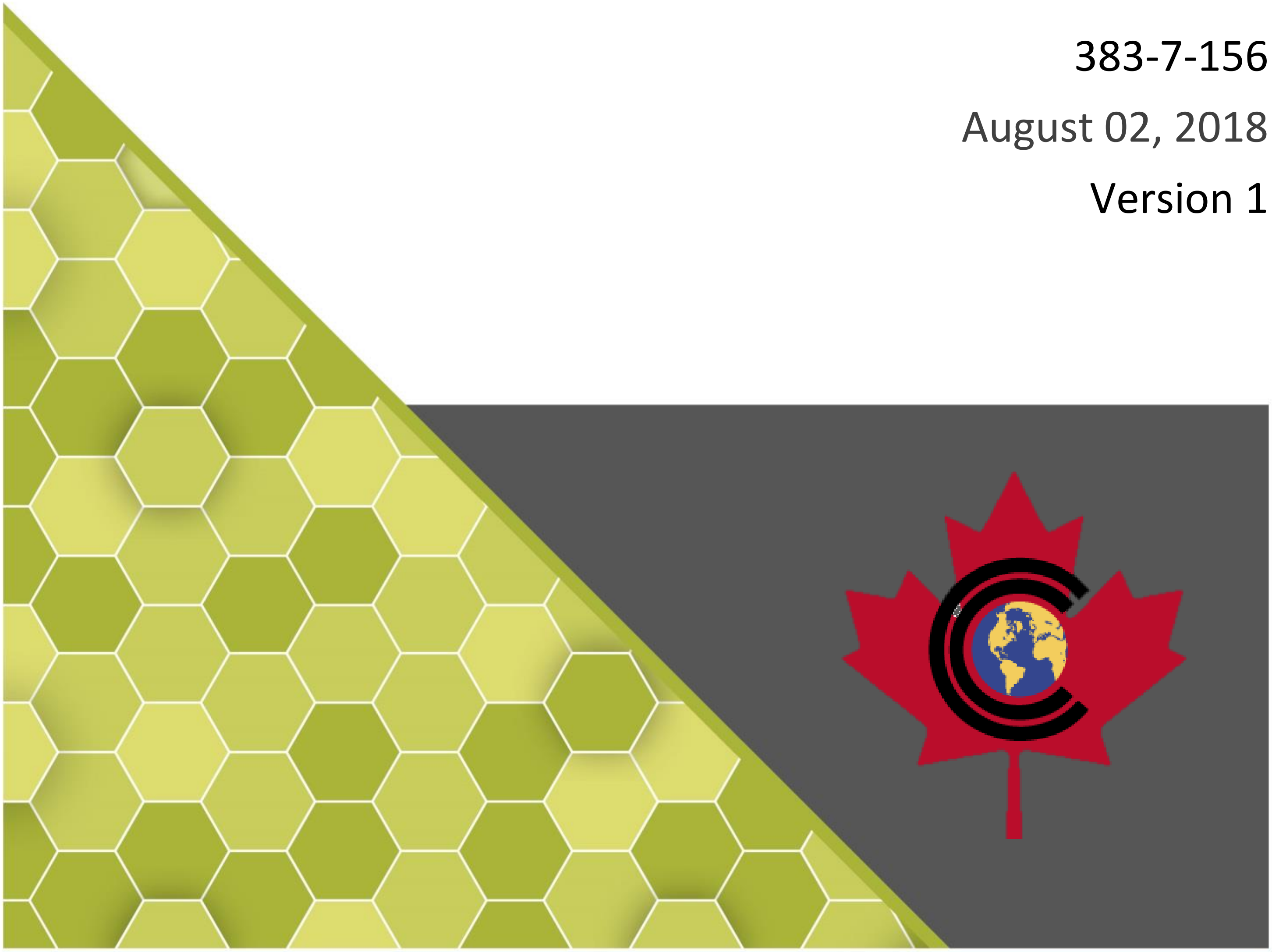
COMMON CRITERIA MAINTENANCE REPORT

Ivanti Patch for Windows Server v9.3 Update 1

383-7-156

August 02, 2018

Version 1



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

Corsec Security Inc. has submitted the Impact Analysis Report (IAR) for Ivanti Patch for Windows Server v9.3 Update 1 (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

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;

- Virtual Machines: VMs are now discoverable;
- Simultaneous Machine Scans: An Administer can now specify the number of simultaneous machines to scan;
- PowerShell API: The PowerShell API is disabled in in this version;
- Folder Paths: Protect Console GUI will display a hierarchical structure for machine groups, patch scan templates, and patch deployment templates, organizing them into folders;
- Staged Deployments: Protect Console GUI gives users more flexibility in scheduling patch deployments;
- Scheduled Snapshot Maintenance: Protect Console GUI gives users the ability to schedule a one-time or recurring task that will remove old VM snapshots from the server;
- Third Party CA: A trusted Certificate Authority can be used to issue a replacement root certificate for Ivanti Patch for Windows Servers;
- New Skins: Allows users to specify a color theme for the Protect Console GUI;
- Scheduled Remote Tasks: Allows users to view tasks scheduled on remote machines by right-clicking on a machine in either Machine View or Scan View and then selecting View scheduled tasks;
- New Column Filter Capabilities: Allows users to apply filters to one or more column headers in the Protect Console GUI grid;
- Manual Download Method: A new Download method column in the Protect Console GUI indicates whether a patch can be downloaded automatically or if it must be downloaded manually;
- Deployment Information: The Deployment Configuration dialog in the Protect Console GUI now shows information about the disk space requirements when deploying patches;
- Consolidated Program Options: All program options in the Protect Console are now consolidated in a single location. They can be viewed from the Protect Console GUI Tools > Options menu;
- Patch Group Filter: The Patch View in the Protect Console GUI contains a new patch group filter that lets users choose whether patches contained in the selected patch group will be displayed in the Patch View list;
- Deployment Tracker: Deployment Tracker in the Protect Console GUI has been redesigned to provide more detail about the patch deployment tasks that are currently in progress;
- Export Download Package: The Protect Console GUI gives users the ability to export the download links for selected patches to a Comma Separated Values (CSV) file;
- New Reports: The Protect Console GUI provides two new IAVA reports: Machine Compliance and Machine Non-Compliance;
- Global Thread Pools: Thread Management has moved from the template level to a system-wide pool and is now defined on the Protect Console GUI Tools > Options > Patch dialog;

- Expanded Search Capabilities: Allows for more search capabilities in the Protect Console GUI;
- Deprecated Feature: Threat management (antivirus and Active Protection) is no longer offered with the product; and
- Unsupported Platforms: The following platforms are no longer supported with Ivanti Patch for Windows Servers v9.3:
  - SQL Server 2005 is no longer supported as a database; the new minimum is SQL Server 2008;
  - The following platforms are no longer supported for use with agents:
    - Windows XP;
    - Windows Server 2003; and
    - Windows Server 2008 R2 Gold.

1.2 DESCRIPTION OF CHANGES TO THE IT ENVIRONMENT

The changes to the IT environment comprise;

- A change to the version of .NET Framework used on the Protect Console hardware, which is located in the TOE environment. The version changed from 4.5.1 to 4.6.2; and
- Added the requirement for Microsoft Visual C++ 2015 (x64), which is located in the TOE environment.

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 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
Common Criteria Certification Report, Shavlik U.S. Federal Protect Standard v9.2 Update 3, Version: 1.0, 8 June 2017
Ivanti Patch for Windows Servers v9.3 Update 1 Security Target Version 1.0, June 24, 2018