Maintenance Report

Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-7-MR
Version: 1.0
Date: 15 September 2005
Pagination: 1 to 3

1 Introduction

On 13 September, Electronic Warfare Associates-Canada (EWA-Canada) submitted an Impact Analysis Report to the CCS Certification Body on behalf of Check Point Software Technologies Incorporated, the developer of the Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14 product. The Impact Analysis Report is intended to satisfy requirements outlined in version 1.0 of the Common Criteria document CCIMB-2004-02-009: Assurance Continuity: CCRA Requirements. In accordance with those requirements, the Impact Analysis Report (IAR) describes the changes made to Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14 (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes

The product name has changed from the VPN-1/FireWall-1 Next Generation to the VPN-1/FireWall-1 Next Generation AI. The changes listed in the IAR include changes made from Feature Pack 1 of the Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14 to R55 with HFA_14.

The following characterizes the changes implemented in the Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14. 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. The changes in Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14 comprise software changes that:

- restore the expected functionality of the product (bug fixes);

- update third party components included in the product;

- extend some insufficient limits of TOE features; and

- add functionality to portions of the product not included in the scope of the original evaluation;

3 Description of Changes to the IT Environment

Changes to the underlying IT Environment are permissible under assurance continuity provided that the original ST did not levy any SFRs on the elements being changed or added to. A modified ST was provided which included a list of additional operating systems and compatible hardware. Check Point Software Technologies subjected the TOE to complete

regression testing on all platforms. The additional operating systems and compatible hardware are:

Operating Systems:

- Sun Solaris 9.0
- Windows XP
- Windows Server 2003
- SecurePlatform

Compatible Hardware:

- Sun Microsystems Inc., Sun Fire V240 Server
- IBM eServer xSeries 306 Server
- IBM eServer sSeries 346 Server
- IBM ThinkPad X40 Notebook
- Siemens Business Services, 4YourSafety RX100 & RX300S Servers
- Hewlett-Packard, HP ProLiant DL380 Server
- Hewlett-Packard, Compaq nc6230 Notebook

4   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, and revised versions of all affected developer evidence were submitted.

Modifications to the security target were made to reflect the new product name, and version, as well as to include the expanded list of compatible underlying hardware and operating systems.

5   Conclusions

All changes to the TOE were features changes and isolated corrections to the product. Through functional and regression testing of the Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation AI R55 with HFA_14, assurance gained in the original TOE certification was maintained. As all of the changes to the 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.

6   References

Assurance Continuity: CCRA Requirements, CCIMB-2004-02-009, version 1.0, February 2004

Technical Oversight for Assurance Continuity of a certified TOE, version 1.0, 18 June 2004

Certification Report for EAL4 Evaluation of Check Point Software Technologies Incorporated VPN-1/FireWall-1 Next Generation Feature Pack 1