Maintenance Report

IP260, IP265, IP390, IP560, IP1220, IP1260, IP2255 Firewall/VPN Appliances with IPSO v4.1 and Check Point VPN-1/FireWall-1 NGX (R60)

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-13-MR
Version: 1.0
Date: 10 November 2006
Pagination: 1 to 2

1 Introduction

On 25 October 2006, Check Point Software Technologies Ltd. submitted an Impact Analysis Report (IAR) to the CCS Certification Body on behalf of Nokia, the developer of the IP260, IP265, IP390, IP560, IP1220, IP1260, IP2255 Firewall/VPN Appliances with operating system IPSO v4.1, which incorporate the Check Point VPN-1/FireWall-1 NGX (R60).

The Check Point VPN-1/FireWall-1 NGX (R60) represents the target of evaluation (TOE), whereas the IT environment comprises the Nokia IP265, IP390, IP560, IP1220, IP1260 and IP2255 hardware models and the Nokia IPSO v4.1 operating system. The Check Point VPN-1/FireWall-1 NGX (R60) is a previously maintained TOE, having been the subject of assurance maintenance in November 2005.

The IAR 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 IAR describes any changes made to the TOE and/or its IT environment, the evidence updated as a result of the changes, and the security impact of the changes.

2 Description of Changes to the TOE

No changes have been made to the TOE since the previous assurance maintenance step in November 2005.

3 Description of Changes to the IT Environment

Changes to the underlying IT environment are permissible under assurance continuity provided that they do not change the certified TOE. A modified ST was provided which listed the updated operating system and hardware. Check Point Software Technologies Ltd. subjected the TOE to complete regression testing on all platforms. Changes to the IT environment's operating system and hardware are:

Operating System:

- IPSO-v4.1-BUILD016-05.19.2006-052320-1515

Hardware:

- IP390, IP560, IP2255 which are new hardware models; and

• IP260, IP265, IP1220, IP1260 which are hardware models revised to comply with the RoHS Directive [1].

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted. The subset 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 versions.

5 Conclusions

All changes were to the underlying operating system and the underlying hardware. Through functional and regression testing, assurance gained in the original TOE certification was maintained. As all of the changes 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

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

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

3. Certification Report for the EAL4 Evaluation of the Nokia IP130, IP350, and IP380 Firewall/VPN Appliances with Check Point VPN-1/FireWall-1 NG FP2, 16 September 2005.

4. Maintenance Report NOKIA IP260, IP265, IP350, IP355, IP380, IP385, IP1220, IP1260, IP2250 Firewall/VPN Appliances with Check Point Technologies Incorporated VPN-1/FireWall-1 NGX (R60), 16 November 2005.

[1] The RoHS Directive stands for "the restriction of the use of certain hazardous substances in electrical and electronic equipment". This Directive bans the placing on the EU market of new electrical and electronic equipment containing more than agreed levels of lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyl (PBB) and polybrominated diphenyl ether (PBDE) flame retardants.