Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0772-2014-MA-01

Kanguru Defender Elite 200 and Kanguru Defender 2000, firmware version 2.05.10

from

Kanguru Solutions

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0772-2014.

The change to the certified product is at the level of the TOE firmware. The change has no effect on assurance. The identification of the maintained product is indicated by a new firmware version number compared to the certified product. The changes lead to an editorial update of the user guidance.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0772-2014 dated 07 November 2014 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0772-2014.

Common Criteria
Recognition Arrangement

Bonn, 20 January 2015

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the Kanguru Defender Elite 200 and Kanguru Defender 2000, firmware version 2.05.10, Kanguru Solutions, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The Kanguru Defender Elite 200 and Kanguru Defender 2000, firmware version 2.05.10 were changed due to error corrections in the TOE firmware. Configuration Management procedures required a change in the product identifier. Therefore the firmware version number changed from 02.03.10 to 02.05.10.

The changes lead to an editorial update of the user guidance [6, 7, 8] in order to reflect the change in the firmware version number.

Conclusion

The change to the TOE is at the level of the TOE firmware and the guidance documents. The change has no effect on assurance. As a result of the changes the configuration lists for the TOE have been updated [5].

The Security Target was editorially updated [9].

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0772-2014 dated 07 November 2014 is of relevance and has to be considered when using the product.

Additional obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report Kanguru Defender Elite 200 and Kanguru Defender 2000 firmware version 2.05.10, version 1.1, 17 December 2014, Kanguru Solutions (confidential document)

[3] Certification Report BSI-DSZ-CC-0772-2014 for Kanguru Defender Elite 200, Kanguru Defender 2000, Universal Kanguru Local Administrator, v3.2.0.3, Kanguru Remote Management Console, v5.0.2.6, Bundesamt für Sicherheit in der Informationstechnik, 07 November 2014

[4] Security Target BSI-DSZ-CC-0772-2014, Version 1.10, 2014-10-06, Kanguru Defender Security Target, Kanguru Solutions

[5] Configuration lists for the TOE (confidential documents):

a) Configuration list for TOE executables, v1.5

b) Configuration list from Phison, 2014-12-17

c) Configuration list for downgrader description, 2014-12-17

d) Configuration list for Secure FTP, 2014-12-17

e) Configuration list for design evidence, 2014-12-17

f) Configuration list for user documentation, 2014-12-17

g) Configuration list for test evidence, 2014-12-17

h) Kanguru hardware configuration setup file, v1.3

i) Kanguru JIRA Bug Report, 2014-12-17

[6] Evaluated Product User Guide, Version 1.21, 2014-12-04

[7] Kanguru Defender Elite 200 User Manual, Version 1.1.1, 2014-12-04

[8] Kanguru Defender 2000 User Manual, Version 1.1.5, 2014-12-04

[9] Kanguru Defender Security Target, Version 1.11, 2015-01-16, Kanguru Solutions