Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1044-2019-MA-01

secunet konnektor 2.0.0, Softwareversion Release 2.0.37

der

secunet Security Networks AG

SOGIS
Recognition Agreement
für Komponenten bis
EAL 4

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus Assurance Continuity: CCRA Requirements, Version 2.1, Juni 2012 und des Impact Analysis Report (IAR) des Herstellers beurteilt. Die Grundlage für diese Beurteilung war der Zertifizierungsreport, die Sicherheitsvorgaben und der technische Evaluierungsbericht des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter der Zertifizierungs-ID BSI-DSZ-CC-1044-2019 zertifizierten Produkts.

Die Änderung im Vergleich zum zertifizierten Produkt wurden auf der Implementierungsebene und auf der Ebene der Anpassung des Handbuches vorgenommen. Die Identifizierung des geänderten Produkts wird durch eine Erweiterung des Produktnamens im Vergleich zum zertifizierten Produkt angezeigt.

Die Betrachtung der Art der Änderung führt zu der Entscheidung, dass die Änderung als “Minor Change“ eingestuft wird und dass das Maintenance-Verfahren für Zertifikate das sachgerechte Verfahren zur Aufrechterhaltung der Vertrauenswürdigkeit ist.

Die Widerstandsfähigkeit gegen Angriffe wurde im Rahmen dieses Maintenance-Verfahrens nicht neu bewertet. Aus diesem Grunde ist die Vertrauenswürdigkeitsaussage im Zertifizierungsreport vom BSI-DSZ-CC-1044-2019 bei der Verwendung des Produktes heranzuziehen. Nähere Informationen finden sich auf den nächsten Seiten.

Dieser Report ist ein Anhang zum Zertifizierungsreport BSI-DSZ-CC-1044-2019.

Common Criteria
Recognition
Arrangement
Anerkennung nur für
Komponenten bis
EAL 2 und ALC_FLR

Bonn, 06 Juni 2019

Bundesamt für Sicherheit in der Informationstechnik

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

Beurteilung

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus Assurance Continuity: CCRA Requirements [1] und des Impact Analysis Report (IAR) [2] beurteilt. Die Grundlage für diese Beurteilung war der Zertifizierungsreport des zertifizierten Produktes (Evaluierungsgegenstand, EVG) [3], die Sicherheitsvorgaben und der technische Evaluierungsbericht wie in [3] angegeben.

Der Vertreiber für secunet konnektor 2.0.0, Softwareversion Release 2.0.37, secunet Security Networks AG, legte dem BSI einen IAR [2] zur Entscheidung vor. Der IAR dient der Erfüllung, der in dem Dokument *Assurance Continuity: CCRA Requirements* [1] angegebenen Anforderungen. In Übereinstimmung mit diesen Anforderungen beschreibt der IAR (i) die am zertifizierten EVG vorgenommenen Änderungen, (ii) die aufgrund der Änderungen aktualisierten Unterlagen und (iii) die Auswirkungen der Änderungen auf die Sicherheit.

Der secunet konnektor 2.0.0, Softwareversion Release 2.0.37 wurde aufgrund einer Anpassung des MTU Wertes auf der internen Netzwerkschnittstelle für bessere Performance, Anpassung am Mechanismus zum Bereinigen interner Subscriptions, Anpassung der Inputvalidierung bei Eingabe von IP Bereichen für VPN_TI_NET und VPN_SIS_NET gemäß gematik-Spezifikation, Korrektur der Anzeige der Seriennummer in der Benutzeroberfläche, Nachbesserung in der Code- bzw. REST-Schnittstellen-dokumentation ohne Auswirkungen auf die Sicherheitsfunktionalität der Schnittstelle sowie kleinere funktionale Anpassungen ohne Auswirkungen auf die Sicherheitsfunktionalitäten geändert. Die Änderungen am Prozess der sicheren Auslieferung betreffen die Auslieferung vom Fertiger per Großtransport zu nun verschiedenen Großlagern oder mittleren Lager sowie die ergänzende Angabe der ICCSN von der gSMC-K in den Versandinformationen bis einschließlich DVO (Dienstleister vor Ort). Die Konfigurations-management-Prozeduren erfordern eine Änderung der Bezeichnung des Produktes. Aus diesem Grunde wurde der Name des Produkte um den Zusatz, Softwareversion Release 2.0.37, erweitert.

Die Sicherheitsvorgaben [5] wurden editoriell aktualisiert.

Die Änderungen bewirkten eine entsprechende Aktualisierung des Handbuches [6].

Schlussfolgerung

Die Änderung des EVG wurde auf der Implementierungsebene und auf der Ebene der Anpassung des Handbuches vorgenommen. Die Änderung hat keine Auswirkungen auf die Vertrauenswürdigkeit, jedoch muss das aktualisierte Handbuch befolgt werden.

Die vom BSI anerkannte Prüfstelle, SRC GmbH, hat die am EVG vorgenommenen Änderungen bewertet. Die Prüfstelle kommt zu dem Schluss, dass es sich bei den Änderungen um „Minor Changes“ handelt und dass das Maintenance-Verfahren für Zertifikate das sachgerechte Verfahren zur Aufrechterhaltung der Vertrauenswürdigkeit ist, siehe [4].

Die Widerstandsfähigkeit gegen Angriffe wurde im Rahmen dieses Maintenance-Verfahrens nicht neu bewertet. Aus diesem Grunde ist die Vertrauenswürdigkeits-aussage im Zertifizierungsreport BSI-DSZ-CC-1044-2019 bei der Verwendung des Produktes heranzuziehen.

Zusätzliche Auflagen und Hinweise für die Verwendung des Produkts:

Alle in den Sicherheitsvorgaben beschriebenen Aspekte der Anforderungen, Bedrohungen und organisatorischen Sicherheitspolitiken, welche nicht vom EVG abgedeckt werden, müssen von der Einsatzumgebung erfüllt werden.

Der Kunde beziehungsweise der Benutzer des Produkts muss die Zertifizierungsergebnisse im Rahmen des bei ihm realisierten Risikomanagement-prozesses individuell bewerten. Um der Weiterentwicklung von Angriffsmethoden und -techniken entgegenzutreten, sollte der Kunde eine Zeitspanne definieren, ab der eine Neubewertung des EVGs erforderlich ist und daher vom Sponsor des Zertifikats verlangt werden wird.

Ergänzender Hinweis: Die Stärke der kryptographischen Algorithmen wurde im Rahmen der Basiszertifizierung und im Rahmen dieses Maintenanceverfahrens nicht bewertet (vgl. § 9 Abs. 4 Nr. 2 BSIG[1])

Für Details zu den Evaluierungsergebnissen zu kryptographischen Aspekten siehe Zertifizierungsreport [3], Kapitel 9.2.

Dieser Report ist ein Anhang zum Zertifizierungsreport [3].

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

Referenzen

[1] Common Criteria Document “Assurance Continuity: CCRA Requirements”, Version 2.1, Juni 2012

[2] Modularer Konnektor 2.0.0, Risiko- und Auswirkungsanalyse (Änderungen), Version 1.3, 08.01.2019 (vertrauliches Dokument) und

Modularer Konnektor 2.0.0, Risiko- und Auswirkungsanalyse (Änderungen) AK, Version 0.8_Rev1, 14.05.2019 (vertrauliches Dokument), sowie zugehörige Patch-Datein „Risiko- und Auswirkungsanalyse_AK_1.0.7-1.0.8_v08_Rev1.zip“

[3] Zertifizierungsreport BSI-DSZ-CC-1044-2019 für secunet konnektor 2.0.0, Bundesamt für Sicherheit in der Informationstechnik, 25.01.2019

[4] Bewertung zu secunet konnektor 2.0.0 Release 2.0.37 und Änderungen an sicherer Auslieferung durch die Prüfstelle SRC GmbH, 15.05.2019

[5] Security Target secunet konnektor 2.0.0, Version 1.5, 16.04.2019, secunet Security Networks AG

[6] secunet Konnektor, Version 2.0.0, Hinweise zur sicheren Lagerung und Lieferkette, Version 1.8, 11.02.2019

[7] Konfigurationsliste

- secunet(konnektor Version 2.0.0 Referenzen, Version 2.0, 15.05.2019
- ALC_CMS_eHX_v2.0.ods
- 190514_ALC_CMS_Modularar-Konnektor_NK-Implementierung_v1.3.xlsx