Bundesamt
für Sicherheit in der
Informationstechnik

# Assurance Continuity Maintenance Report

## BSI-DSZ-CC-1044-2019-MA-02

## secunet konnektor 2.0.0, Softwarestand 2.0.38

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, aktualisiert durch ein vorheriges Maintenance-Verfahren am 6. Juni 2019.

Die Änderung im Vergleich zum zertifizierten Produkt wurde auf der Ebene von dem Sicherheits-Log-Mechanismus 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.

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

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

Bonn, 19 September 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 die technischen Evaluierungsberichte wie in [3] angegeben.

Der Vertreiber für secunet konnektor 2.0.0, Softwarestand 2.0.38, 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, Softwarestand 2.0.38 wurde aufgrund von folgenden Anpassungen geändert:

- Eine Anpassung des Firewall-Regelwerks durch Hinzufügen einer weiteren Regel, die Broadcast-Pakete, die aus dem LAN empfangen werden, fallen lässt, ohne diese im Sicherheits-Log zu protokollieren.
- Ein überflüssiger Transaktionsmechanismus im Logging-Mechanismus wird nicht mehr verwendet.
- Die Datenbankabfragen zum Löschen älterer Logeinträge beim Rollieren wurde umgestellt:
  - Berücksichtigung der angepassten Spezifikationsanforderung [7] bzgl. Gewichtung der Fehler-Einträge beim Löschen.
  - Es werden 100 ältere Einträge auf einmal gelöscht, um genügend freie Einträge als Puffer zu schaffen.

Die Konfigurationsmanagement-Prozeduren erfordern jedoch eine Änderung der Bezeichnung des Produktes. Aus diesem Grunde wurde der Name des Produkts um den Zusatz, Softwarestand 2.0.38, erweitert.

Die Sicherheitsvorgaben [6] wurden editoriell aktualisiert.

# Schlussfolgerung

Die Änderung des EVG wurde auf der Implementierungsebene vorgenommen.

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 Risikomanagementprozesses 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[2])

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

Dieser Report ist ein Anhang zum Zertifizierungsreport [3].

2 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 1.4.1, 03.04.2019 (vertrauliches Dokument), sowie zugehörige Patch-Dateien „PATCHES-37-38.zip“

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

und

Maintenancereport BSI-DSZ-CC-1044-2019-MA-01 für secunet konnektor 2.0.0, Softwareversion Release 2.0.37, Bundesamt für Sicherheit in der Informationstechnik, 06.06.2019

[4] Bewertung zu secunet konnektor 2.0.0 Release 2.0.38 durch die Prüfstelle SRC GmbH, 15.05.2019

[5] Konfigurationsliste

Referenzen, Version 2.2, 24.05.2019

ALC_CMS_eHX_v2.0.ods

190514_ALC_CMS_Modularar-Konnektor_NK-Implementierung_v1.4.xlsx

[6] Security Target für secunet konnektor, Version 1.6, 16.04.2019

[7] Spezifikation Konnektor, Version 5.4.0, 26.10.2018, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH