Genuscreen 7.0

EAL4.

Description of the product: genuscreen 7.0 has two main functions – firewall and VPN. It uses the firewall function to monitor data traffic at critical network interfaces and tIt protecs the LAN/Internet interface from cyber attacks by allowing only expressly autorized connections. It can also monitor crossover points to internal high-security zones in large networks. The VPN function enables exhcanging encrypted data between spread out company locations or public autority sites over the internet (https://www.genua.de/en/news/presse/2019/genuscreen-certification.html)

The product consists only of the sofware (in a CD or a USB stick) and the documentation. One part of the product runs on a number of (at least 2) machines (genuscreen appliances) and works as network filters . The other part runs on the machine to manage the network of firewall components (genucenter management system) is the central component. Genuscreen provides IPv4 and basic IPv6 support. The product contains cryptographic functionality. The cryptographic algorithms are part of the TOE. This includes the random number generator which is of class DRG.3 The vulnerability assessment results as stated within this certificate do not include a rating or those cryptographic algorithms and their implementation suitable for encryption and decryption.

Non-TOE components of the product:

- genucenter Management System:
- genuscreen Firewall Components:
- Legacy Hardware and Virtual genucenter

Security Assurance Rationale

ALC_FLR.2 Flaw reporting procedures
ASE_TSS.2 TOE summary specification with architectural design summary
AVA_VAN.4 Methodical vulnerability analysis

Security Functional Requirements claimed by TOE

- **Firewall SFP**: concerned with the creation, modification, deletion and application of firewall security policy rules; it also provides protaction against unauthorized access to the platform running the firewall components
- **Network Separation SFP**
- **IPSec SFP:** including requirements on some cryptographic operations
- **IKE SFP:** cryptographic functions in relations to the key management of the VPN connections
- **SSH SFP:** requirements associated with the flow control functions in relation to the communication between the management system and the firewall components, (includes cryptographic operations)
- **SIP Relay**
- **Identifiaction and Authentication:** related to identification and authentication of administrators, service users and revisors.
- **Audit:** audit capabilities of the TOE
- **General Management Facilities**

Assumptions

The TOE assumes the following:

- Physical security
- Initial configuration

- Responsible, competent and trained administrators, service users and revisors
- Firewall components provide the only connection for different networks
- The IT environment must supply reliable timestamps for the TOE
- Administrators, service users and revisors use the administrative GUI only from a trusted network directly connected to the system, they log in with SSH only from this network and use SSH keys but no passwords to authenticate
- Physical network for transfer of TSF data between nodes is provided.
- Server for external authentication at the genucenter is located in a secure network

Evaluation

The product was tested in the developer's laboratory and also by an independent evaluator. The test procedures are executable scripts (Ruby, Perl or Shell). The developer uses two kinds of tests: Local tests and Live tests. Local tests need the developer environment and were executed inside the developer systems. Prior the testing by the independent evaluator, the evaluator installed the firewall components in a separate administrator network. During the test, was the main focus the implemented SIP Relay, the management system, cryptographic functions, random number generator (RNG) and its entropy source (part of OpenBSD kernel) functions. The repetition of the developer testing was performed in the developer laboratory. -also, the evaluator has done an independent vulnerability analysis. As a result, additional vulnerability tests have been designed.