Ympäristö	Järjestelmä	Haavoittuvuus	CVSS
Kaikki ympäristöt	Greenbone Vulnerability Management	Vanhentunut ohjelmistoversio	10.0
WS-NET	DCE/RPC ja MSRPC	Palveluiden luettelointi	5.0
WS-NET	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4.3
Admin-Net	ICMP	Aikaleima-vastausten tietovuoto	2.1
Servers-Net	DCE/RPC	Palveluiden luettelointi	5.0
Servers-Net	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4.3
DMZ	SSH	Heikko avaintenvaihtoalgoritmi	5.3
DMZ	SSL/TSL	SSL/TLS alttius DoS hyökkäyksille	5.0

DMZ	SSL/TSL	Tuntemattoman tai vaarallisen varmenteen myöntäjän havaitseminen	5.0
DMZ	SSL/TSL	Sertifikaatti on vanhentunut	5.0
DMZ	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4.3
DMZ	SSH	Heikkojen salausalgoritmien tuki (SSH)	4.3

CVE	Korjaus / lievennysehdotus
-	Päivitä lisenssi uudempaan versioon
-	Suodata portteihin tulevaa liikennettä
CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
CVE-199-0524	Estä tarpeettomat ICMP-vastaukset tai konfiguroi palomuuri suodattamaan pyyntöjä
-	Suodata portteihin tulevaa liikennettä
CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
-	Poista käytöstä raportoidut heikot avaintenvahitoalgoritmit (KEX). Käytä vaihtoehtoisesti elliptistä käyrää hyödyntävää Diffie-Hellman -avaintenvaihto, esimerkiksi Curve 25519
CVE-2011-1473, CVE-2011-5094	Ota yhteys palveluntarjoajaan. Poista/ota pois käytöstä uudelleenneuvotelupyynnöt SSL/TLS palveluilta.

-	Varmenteen vaihtaminen sellaiseen jonka myöntäjä on luotettu
-	Uusi kaikki vanhentuneet varmenteet.
CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
-	Ota käyttöön vahvemmat salausalgoritmit kuten AES-256,ChaCha20