

Ympäristö	Järjestelmä	Haavoittuvuus	CVSS	CVE	Korjaus / lievennysehdotus
Kaikki ympäristöt	Greenbone Vulnerability Management	Vanhentunut ohjelmistoversio	10,0	-	Päivitä lisenssi uudempaan versioon
WS-NET	DCE/RPC ja MSRPC	Palveluiden luettelointi	5,0	-	Suodata portteihin tulevaa liikennettä
WS-NET	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4,3	CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
Admin-Net	ICMP	Aikaleima-vastausten tietovuoto	2,1	CVE-199-0524	Estä tarpeettomat ICMP-vastaukset tai konfiguroi palomuuuri suodattamaan pyyntöjä
Servers-Net	DCE/RPC	Palveluiden luettelointi	5,0	-	Suodata portteihin tulevaa liikennettä
Servers-Net	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4,3	CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
DMZ	SSH	Heikko avaintenvaihtovalgoritmi	5,3	-	Poista käytöstä raportoidut heikot avaintenvaihtovalgoritmit (KEX). Käytä vaihtoehtoisesti elliptistä käyrää hyödyntävää Diffie-Hellman -avaintenvaihtoa, esimerkiksi Curve 25519
DMZ	SSL/TSL	SSL/TLS alttiut DoS hyökkäyksille	5,0	CVE-2011-1473, CVE-2011-5094	Ota yhteys palveluntarjoajaan. Poista/ota pois käytöstä uudelleenneuvotelupyynnöt SSL/TLS palveluilta.
DMZ	SSL/TSL	Tuntemattoman tai vaarallisen varmenteen myöntäjän havaitseminen	5,0	-	Varmenteen vaihtaminen sellaiseen jonka myöntäjä on luotettu
DMZ	SSL/TSL	Sertifikaatti on vanhentunut	5,0	-	Uusi kaikki vanhentuneet varmenteet.
DMZ	SSL/TSL	Vanhentuneiden TLSv1.0 and TLSv1.1 Protokollien käyttö	4,3	CVE-2011-3389, CVE-2015-0204	Poistetaan käytöstä TLSv1.0 ja TLSv1.1 protokollat ja korvataan ne TLSv1.2 tai uudemmalla
DMZ	SSH	Heikkojen salausalgoritmien tuki (SSH)	4,3	-	Ota käyttöön vahvemmat salausalgoritmit kuten AES-256,ChaCha20