ISDS přestává akceptovat zastaralé šifrovací sady v protokolu TLS – únor 2020

Datum: 21. 2.2020
Verze: 1

Klasifikace: veřejný dokument

1 Anotace změny

ISDS přestává akceptovat zastaralé šifrovací sady v protokolu TLS, v souladu s doporučením NUKIB ze dne 28.11.2018 Minimální požadavky na kryptografické algoritmy – doporučení v oblasti kryptografických prostředků. Toto opatření může mít dopad na některé velmi staré aplikace, které se připojují k ISDS.

2 Harmonogram změny

V prostředí Veřejného testu ISDS bude změna nasazena 1.3.2020. Na produkčním ISDS bude změna nasazena pravděpodobně v červnu 2020.

3 Popis změny

S ohledem na výše uvedené bude na přístupových bránách ISDS, které terminují TLS spojení, vypnuta podpora pro dané 2 zastaralé šifrovací sady:

- TLS_RSA_WITH_AES_128_CBC_SHA a
- TLS_RSA_WITH_AES_256_CBC_SHA.

Na všech rozhraních nastavena podpora těchto šifrovací sad v preferovaném pořadí:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits

Důvody pro udržování starého seznamu šifrovacích sad, který byl původně vybrán pro zachování maximální kompatibility s klienty ve Windows XP a Java 6 (čili staršími 15 let), už pominuly. Tuto

kompatibilitu už není zapotřebí zajišťovat. Byla přerušena už na podzim 2018, kdy byly v ISDS globálně vypnuty protokoly TLS 1.0 a 1.1.

Pro portálové uživatele změna dopad nemá.

4 Poznámky

Pro ověření funkčnosti se stačí po odstávce 1.3.2020 přihlásit do nějaké schránky v testovacím prostředí ISDS.