Informace pro vývojáře aplikací – červen 2020

Datum: 25. 5.2020
Verze: 1

Klasifikace: veřejný dokument

1 Anotace změny

V souladu s všeobecně doporučovanými postupy zavádí ISDS dvě bezpečnostní úpravy konfigurace webového serveru. Toto opatření může mít dopad na některé velmi staré, neaktualizované aplikace, které se připojují k ISDS.

2 Harmonogram změny

V prostředí veřejného testu ISDS bude změna nasazena **7.6.2020**. Na produkčním ISDS bude změna nasazena pravděpodobně v **září 2020**.

3 Popis změny

3.1 Zavedení OCSP staplinku

Online Certificate Status Protocol (OCSP) stapling, je standardizovaný způsob zprostředkování kontroly platnosti (resp. revokace) certifikátů serverem a spočívá v připojení OCSP odpovědi rovnou k počáteční odpovědi v rámci navázání šifrovaného spojení mezi serverem a prohlížečem. Nahrazuje původní implementaci OCSP přímo v prohlížečích, od které se upustilo, neboť zpomalovala načítání stránek, protože vyžadovala, aby klient kontaktoval třetí stranu (CA) kvůli platnosti každého certifikátu, se kterým se setkal. Pomocí staplingu na místo toho server „přišije“ informaci o platnosti svého vlastního certifikátu přímo ke své odpovědi na klientský požadavek.

Odkaz na specifikaci:

https://tools.ietf.org/html/rfc4366

3.2 Změna pořadí šifrovacích sad

V rámci odstávky bude také změněno pořadí šifrovacích sad. Tato změna v pořadí preferovaných sad umožní v budoucnu jednodušší odstranění dosluhujících sad SHA, neboť klienti automaticky přejdou na silnější šifry – odstranění bude následovat nejspíše v příští odstávce, opět nejprve v prostředí veřejného testu, později na produkčním prostředí ISDS.

Šifrovací sady pro webové služby (ws1.mojedatovaschranka.cz pro produkční prostředí, ws1.czebox.cz pro testovací prostředí) jsou aktuálně (tj. před zde popisovanou změnou) navazovány dle konfigurace, kdy pro klienta server pořadí neurčuje (klient si sadu vybírá sám a server nechává zcela na preferenci klienta, zda naváže spojení pomocí silnější šifrovací sady nebo naopak pomocí slabší šifrovací sady, a to i tehdy, pokud je silnější sada k dispozici).

Servery v ISDS začnou nově uplatňovat níže uvedenou preferenci pořadí. Tak dojde k tomu, že klient při navázání se serverem použije nejsilnější sadu, na které se obě strany dokáží dohodnout.

Na všech rozhraních bude (postupně) nastavena podpora těchto šifrovací sad v preferovaném pořadí:

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

4 Poznámky

Pro ověření funkčnosti se stačí po odstávce 7.6.2020 přihlásit do nějaké schránky v testovacím prostředí ISDS. Pro naprostou většinu aplikací se nic nezmění.