

Marushka

Vyčištění cache prohlížeče - certifikát

Autor	Datum	Verze aplikace
Stanislav Štangl	18.12.2017	1.0



OBSAH

0	BSAH	2
1.	Popis problému	3
	Oprava pro prohlížeč Chrome	4
	Oprava pro prohlížeč Mozilla FireFox	5
	Další možnost – využití anonymního režimu	5

1. Popis problému

Po zavolání mapové aplikace MARUSHKA (např. <u>https://gis.plzen.eu/uzemnisprava/</u>) se objeví chybová hláška o důvěryhodnosti certifikátu:

(j)	Chyba zabezpečeného spojení
	Při spojení s gis.plzen.eu nastala chyba. Server používá key pinning (HPKP), ale nebyl složen vhodný řetězec důvěryhodných certifikátů, které se shodují s daným pinsetem. Porušení key pinning není možné ignorovat. Kód chyby: MOZILLA_PKIX_ERROR_KEY_PINNING_FAILURE
	 Požadovanou stránku nelze zobrazit, protože nelze ověřit autenticitu přijatých dat. Kontaktujte prosím vlastníky webového serveru a informujte je o tomto problému.
	Zjistit více
	✓ Hlásit chyby jako je tato a pomoci tak organizaci Mozilla identifikovat a blokovat škodlivé stránky
	Zkusit znovu

Duvod nahrady certfikatu je popsan zde: https://www.root.cz/clanky/symantec-chyboval-sev-certifikaty-prohlizece-jim-prestanou-duverovat/

Většina webových prohlížečů si s neplatnou hlavičkou certifikátu poradí sama, ale evidjeme jednotky případů, kdy se tak nestalo. Pro každý prohlížeč (IE, Mozillu nebo Google Chrome) se to chová různě. A proto použijte následující postup dle svého prohlížeče.

Oprava pro prohlížeč Chrome

V Chrome na adresní řádek zkopírujte

chrome://net-internals/#hsts

Otevře se okno s nastavením, ve kterém se dá ověřit, zda je doména cachovaná a pokud ano, úplně dole je nutné ji vymazat:

Pokud je v řádku Domain (viz obrázek níže) text *"plzen.eu*" nebo *"gis.plzen.eu*" stisknutím tlačítka **Delete** dojde k jejímu smazání.

capturing events (62559)		
Capture		
Import HSTS/PKP		
Proxy HSTS is HTTP Strict Transport Security: a way for sites to elect to always use HTTPS. See <u>https://www.chromium.org/hsts</u> . PKP is Public Key Pinning: a w	ay for sites to	
Events Add HSTS/PKP domain		
DINS input a domain name to add it to the HSTS/PKP set:		
Alt-SVC		
HTTP/2 Include subdomains for PKP:		
OUIC Public key fingerprints:		
SDCH (public key fingerprints are comma separated and consist of the hash function followed by a foreslash and the base64 encoded fingerpr	nt, for exam	
Cache Add		
Modules		
Domain Security Policy Query HSTS/PKP domain		
Bandwidth Input a domain name to query the current HSTS/PKP set:		
Prerender Domain: plzen.eu Query		
Not found		
Expect-CT		
Expect-CT allows sites to elect to always require valid Certificate Transparency information. See https://tools.ietf.org/html/draft-ietf-httpbis-expect-ct.		
Add Expect-CT domain		
Input a domain name to add it to the Expect-CI set. Leave Enforce unchecked to configure Expect-CI in report-only mode.		
Domain: example.com		
Report URI (optional): https://reporting.example.com		
Add		
Query Expect-CT domain		
Input a domain name to query the current Expect-CT set:		
Domain: example.com		
Delete densis services Pre-		
Delete domain security policies		
Input a domain name to delete its dynamic domain security policies (HSTS, HPKP, and Expect-CT). (you cannot delete preloaded entries):		
Domain: example.com Delete		

Oprava pro prohlížeč Mozilla FireFox

Pro Mozillu jsme objevili řešení na stránce:

https://linux-audit.com/deleting-outdated-hpkp-key-pins-in-firefox/

V podstatě je potřeba nejprve zavřít Mozillu a pak se podívat do adresáře něco.default (může mít různý řetězec před .default), který by se měl v PC nacházet na cestě C:\Users\JMÉNO UŽIVATELE\AppData\Local\Mozilla\Firefox\Profiles\ (pozor – adresář AppData bývá obvykle skrytý).

V tomto adresáři by neměl být žádný *.txt soubor. Pokud tam nějaký je (např. SiteSecurityServiceState.txt), tak by se měl odstranit. Pak by to již mělo fungovat.

Další možnost – využití anonymního režimu

Lze použít anonymní režim (FF i Chrome), ten nesahá do uložených dat, ale je to pouze workaround.