

HTTPS zdarma a pro všechny



Ing. Tomáš Hála
Linux Teamleader
ACTIVE 24, s.r.o.
@tomashala

10. října 2015
LinuxDays 2015



A proč?


Proč bychom měli šifrovat i stránky, ke kterým se nepřihlašujeme?



HTTPS BY MĚLO BÝT VŠUDE



Celý internet směřuje k šifrování. Bezpečnostních kauz přibývá a s nimi se násobí úsilí rozšířit i šifrování mezi uživatelem a službami. HTTPS by se mělo stát standardem, který bude nejen očekáván, ale i vyžadován na mnoha úrovních: od prohlížečů až po uživatele. Výsledkem bude lepší web pro všechny.

 23. 9. 2015 0:00 [Petr Krčmář](#)
 [Našli jste v článku chybu?](#)

AUTOR ČLÁNKU


Petr Krčmář  

Petr Krčmář pracuje jako šéfredaktor serveru Root.cz.

Studoval elektroniku a média, takže je rozpolcen mezi dva obory. Snaží se dělat obojí, jak nejlépe umí.

Psali to na rootu. Před dvěma týdny a celkem zevrubně. Předpokládám, že jste všichni četli, tedy..

Děkuji za pozornost!

(Pokud jste to náhodou nečetli nebo chcete vědět více, poslouchejte dále a třeba se dozvíte něco nového.)



```
root@home:~# curl -I https://www.root.cz/  
HTTP/1.0 301 Moved Permanently  
Location: http://www.root.cz/  
Content-Type: text/html  
Content-Length: 156
```

Root sám před pár dny HTTPS zprovoznil. Zatím jen takto, ale dá se předpokládat, že brzy na něj přejde na ostro.

Dobře, tak co jsou ty důvody?

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.
May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Dle RFC 7258 máme všudypřítomné sledování považovat za útok a snažit se mu bránit a omezovat možnosti odposlechu už v samotných přenosových protokolech.

Nečtu nic tajného, mně šmírování nevadí..

Ne každému to vadí, že je jeho aktivita na internetu sledována (např. zaměstnavatelem nebo reklamními agenturami). Jaké jsou tedy další důvody?





“Eric” “Mill”

@konklone



+ Sledovat


Wikipedia's decision to enforce HTTPS is now pitting them against Russian censors, who want the HTTPS turned off:





theguardian.com/world/2015/aug...



Zobrazit překlad

The screenshot shows the Russian Wikipedia homepage. On the left is a navigation menu with links: Заглавная, Рубрикация, Указатель А — Я, Избранные статьи, and Случайная статья. The main content area features a large globe with the text: Добро пожаловать в Википедию, свободную энциклопедию, которую может редактировать каждый. Сейчас в Википедии 1 248 170 статей на русском языке. Below this is a button: Создать статью (с помощником). At the bottom, there is a news snippet: Russia briefly bans Wikipedia over page relating to drug use. Court ordered ban on page about charas, an Indian form of hashish, but some Russian users found entire site blocked due to secure https protocol. theguardian.com

Wikipedia se po zavedeni HTTPS dostala do křížku s ruskými cenzory – nemohli zablokovat konkrétní stránku a žádali odstranění HTTPS. Úřady udržují seznamy stránek, na které všichni lokální poskytovatelé připojení blokují přístup.

 **“Eric” “Mill”** @konklone · 26. 8.
Wikipedia's decision to enforce HTTPS is now pitting them against Russian censors, who want the HTTPS turned off: theguardian.com/world/2015/aug...

  169  66  [Zobrazit souhm](#)

 **Faidon Liambotis** @faidonl  [+ Sledovat](#)

@konklone The fun part of course is that with HSTS at 1y and preloaded into browsers, we couldn't "turn it off" even if we wanted to :)

Se zapnutým HSTS (více později) a preloadem v prohlížečích už ale vypnutí HTTPS není ani technicky možné a tedy není možné ani blokovat či modifikovat části obsahu.

To je Rusko, u nás přece cenzura nehrozí..

Dobře, zasahovat do obsahu stránek se mi nelíbí, ale u nás přece není cenzura jako v Rusku, my máme přístup na internet bez regulace státní správou.



Hlava II
Nepovolené internetové hry

§ 82
Blokace nepovolených internetových her

(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her“).

Právě v těchto dnech projednávaný návrh novely zákona o hazardních hrách ale navrhuje přesně takový druh regulace a otevírá Pandořinu skříňku. Chceme, aby ministerstvo určovalo, jaké stránky si smíme prohlížet a jaké ne?

Hmm, a to je jako vše?

Jsou tedy šmírování a cenzura jediné
důvody pro nasazování HTTPS?

active 24

How?

Exploit the target transparently by injecting a browser-based exploit while he's surfing the web (http)

]HackingTeam[

Ve známé kauze HackingTeam se v plné nahotě ukázalo, jak se infikují počítače obětí malwarem – útočný kód se vkládá po cestě do jinak zcela legitimních webových stránek fungujících na nešifrovaném HTTP, když je oběť navštíví.

Hacking Team Flash Zero-Day Linked to Cyber Attacks on South Korea and Japan

📅 Thursday, July 09, 2015 👤 Wang Wei

 121  2.5k  962  226  11  1405



Využívali k tomu např. 0-day zranitelnost ve Flash Playeru.



The Hacker News™

Security in a serious way

Second Flash Player Zero-day Exploit found in 'Hacking Team' Dump

📅 Saturday, July 11, 2015 👤 Swati Khandelwal

189

Like 2.3k

Share 1703

Tweet 452

Share 17

ShareThis 2478



A ne jednu..

[« Back to Articles](#)

Hacking Team, the third Flash Zero-Day is out: CVE-2015-5123

[securityaffairs.co](#) - 3 months ago - by Pierluigi Paganini

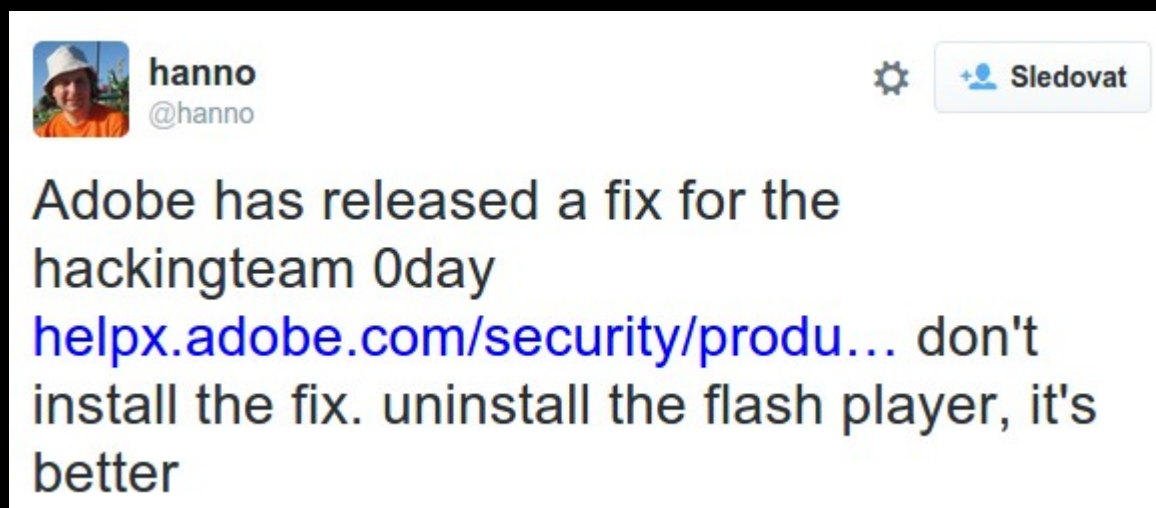
Following the Hacking Team data breach, the security researchers discovered the third Adobe Flash Player zero-day vulnerability. A third Adobe Flash Player zero-day has been discovered since the Hacking Team breach. Thanks to the breach of the Hacking Team's private files, the third Adobe Flash zero-day has been made publicly accessible.

"After two Adobe Flash player zero-days disclosed in a row from the leaked data of Hacking Team, we discovered another Adobe Flash Player zero-day (assigned with CVE number, CVE-2015-5123) that surfaced from the said leak. Adobe has already released a [security advisory](#) after we reported the said zero-day. This vulnerability is rated as critical and can allow an attacker to take control of the affected system once successfully exploited. It affects all versions of Adobe Flash in Windows, Mac, and Linux." reported a [blog post](#) from Trend Micro. This newly uncovered zero-day has a similar PoC as the one released immediately prior...(continued)



[View Full Original Article](#)

Ani ne dvě a samozřejmě ne jen ve Flashi. Měli připravené zranitelnosti prakticky pro jakoukoliv běžně používanou platformu na počítačích, tabletech nebo mobilech.



Když už jsme u toho Flashe, Adobe nalezené díry s odstupem času záplatuje, ale neinstalujte je – Flash prostě odstraňte. Vážné díry se v něm objevují stále dokola a je již přežitý. Stejně se v něm dnes zobrazuje zejména reklama.

Proč by po mně šel nějaký HackingTeam?

Malware ve svém mobilu/tabletu/počítači nechcete, ale proč by právě po vás šel nějaký HackingTeam nebo PČR, která používá jejich SW?

Nemusí, stačí že používáte Wi-Fi..



Tato krabička za \$99 zjistí, k jakým Wi-Fi sítím je vaše zařízení ochotno se připojit a obratem takovou vytvoří. Na nic neklikáte, nic nepotvrzujete, stačí být jen v její blízkosti. Následně lze provádět všechny myslitelné MITM útoky.



[Home](#)
[Chromium](#)
[Chromium OS](#)

Quick links

[Report bugs](#)
[Discuss](#)
[Sitemap](#)

Other sites

[Chromium Blog](#)
[Google Chrome Extensions](#)
[Google Chrome Frame](#)

Except as otherwise [noted](#), the content of this page is licensed under a [Creative Commons Attribution 2.5 license](#), and examples are licensed under the [BSD License](#).

[Chromium](#) > [Chromium Security](#) >

Marking HTTP As Non-Secure

Proposal

We, the Chrome Security Team, propose that user agents (UAs) **gradually change their UX to display non-secure origins as affirmatively non-secure**. We intend to devise and begin deploying a transition plan for Chrome in 2015.

The goal of this proposal is to more clearly display to users that HTTP provides no data security.

Request

We'd like to hear everyone's thoughts on this proposal, and to discuss with the web community about how different transition plans might serve users.

Background

We all need data communication on the web to be secure (private, authenticated, untampered). When there is no data security, the UA should explicitly display that, so users can make informed decisions about how to interact with an origin.

Roughly speaking, there are three basic transport layer security states for web origins:

- **Secure** (valid HTTPS, other origins like (*, localhost, *));
- **Dubious** (valid HTTPS but with mixed passive resources, valid HTTPS with minor TLS errors); and
- **Non-secure** (broken HTTPS, HTTP).

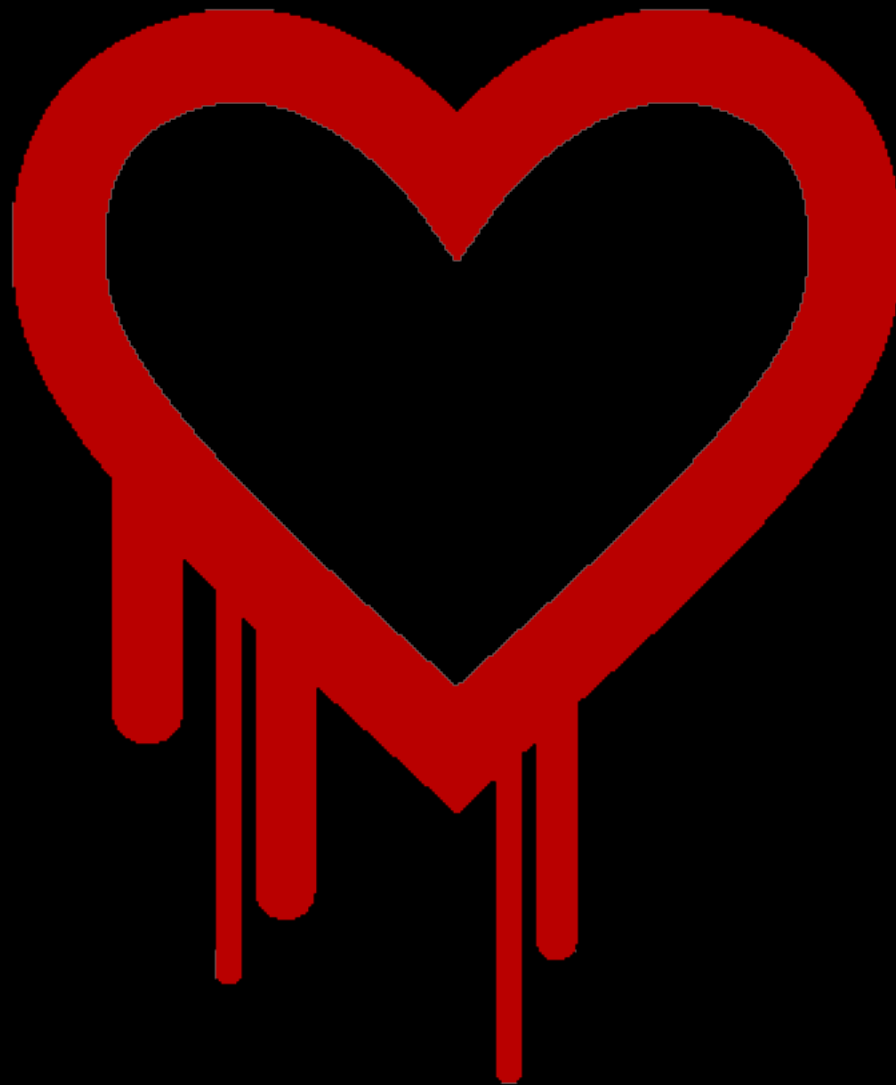
For more precise definitions of *secure* and *non-secure*, see [Requirements for Powerful Features](#) and [Mixed Content](#).

Řešením by bylo, kdyby prohlížeče používaly jen HTTPS. Chrome dnes zvýrazňuje weby, které mají na HTTPS slabý certifikát. Paradoxně ale neoznačuje weby, které nemají vůbec žádné zabezpečení. Zřejmě je to ale jen otázka času.

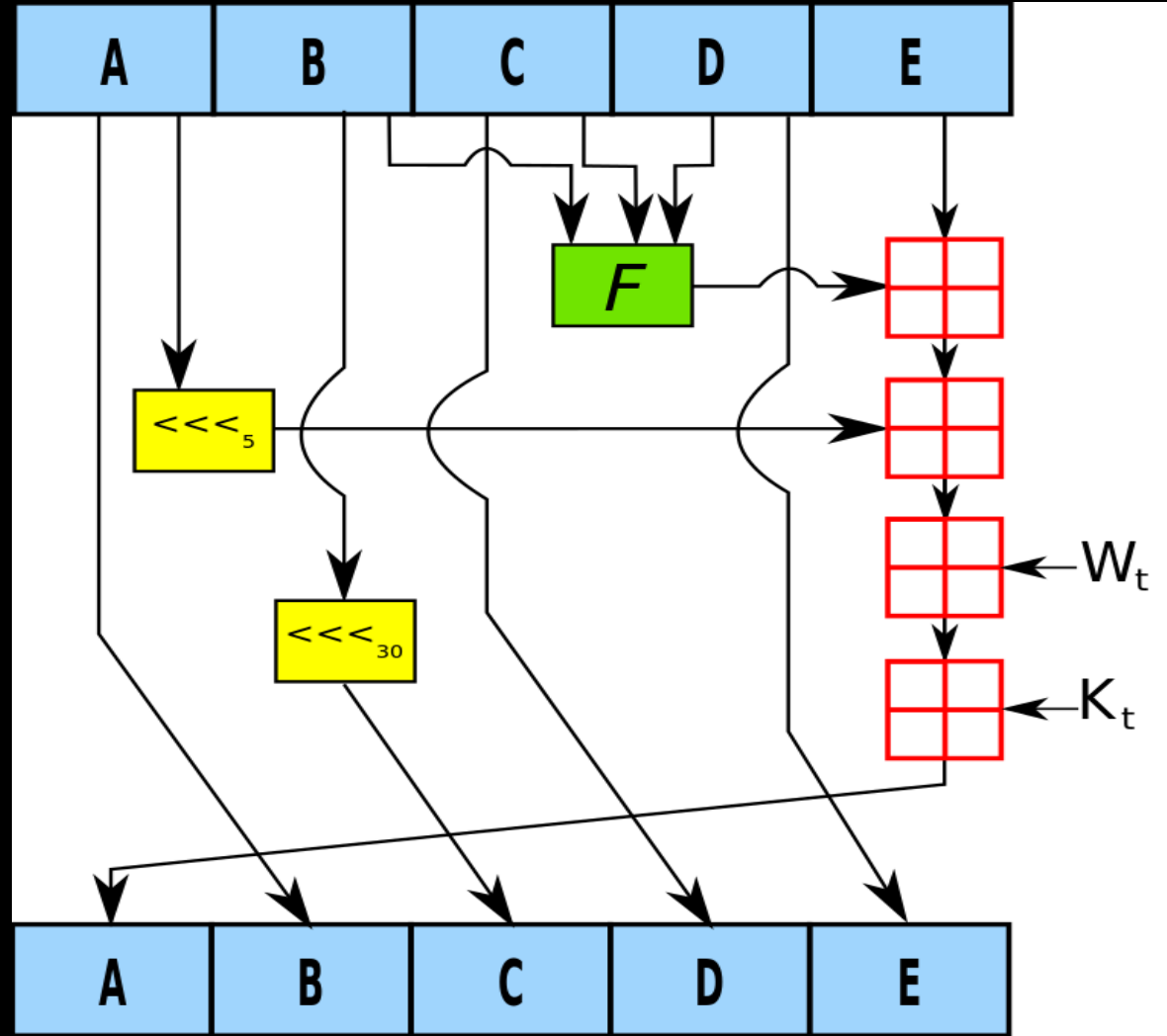
Vždyt' SSL je také plné chyb..

I v SSL implementacích, protokolech a šifrovacích algoritmech jsou chyby a slabiny. Pojd'me se podívat na několik těch nedávných.

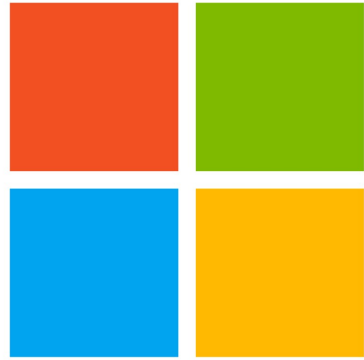




Bezprecedentní chyba HeartBleed v OpenSSL umožňovala vzdáleně získat fragmenty paměti serveru a tedy i privátní klíč komunikace a to bez jakékoliv stopě po této aktivitě. Kromě záplatování bylo nutné vyměnit certifikáty včetně klíčů.



Algoritmus SHA-1, který byl nejrozšířenějším algoritmem pro ověřování SSL certifikátů, je dnes již slabý a nelze ho považovat za bezpečný. Nahrazuje se algoritmem SHA-256. Weby s SHA-1 certifikátem jsou označovány jako nezabezpečené. Kdo tedy po HeartBleed nasadil nový SHA-1 certifikát, mohl jej měnit znovu.



SChannel

Chyby se nevyhýbaly ani komerčním platformám. SSL implementace ve Windows (SChannel) obsahovala závažnou remote-code-execution chybu.



Chyba POODLE se netýkala implementace, ale samotného SSL 3.0 protokolu, který byl sice starý, ale stále hojně užívaný. Po zveřejnění se tato verze protokolu velice rychle přestala používat. (Kéž by stejně rychle zmizel Flash po kauze HackingTeam..)

The Logjam Attack

Warning! Your web browser is vulnerable to Logjam and can be tricked into using weak encryption. You should update your browser.

Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, IPsec, SMTPS, and protocols that rely on TLS.

We have uncovered several weaknesses in how Diffie-Hellman key exchange has been deployed:

Útok nazvaný Logjam využíval zranitelností v implementacích výměny klíčů metodou Diffie-Hellman. Kromě HTTPS se týká i protokolů jako SSH nebo různé VPN implementace. Bylo nutné aktualizovat SW tak, aby mohl používat delší a náhodně generované DH parametry.

Internet Engineering Task Force (IETF)
Request for Comments: 7465
Updates: [5246](#), [4346](#), [2246](#)
Category: Standards Track
ISSN: 2070-1721

A. Popov
Microsoft Corp.
February 2015

Prohibiting RC4 Cipher Suites

Abstract

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections. This applies to all TLS versions. This document updates RFCs 5246, 4346, and 2246.

V hojně využívané šifrovací sadě RC4 bylo nalezeno několik slabín, a tak byla tato šifra označena jako slabá a nevhodná k zabezpečení komunikace.

OK, tak jak to správně nastavit?

Když je v SSL tolik chyb, jak to tedy nastavit a kde zjistím, že to mám nastaveno správně?

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [active24.cz](#) > 2a02:4a8:ac24:100:0:0:96:6

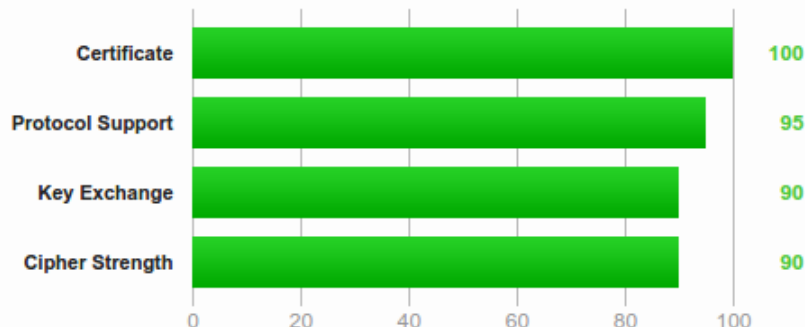
SSL Report: [active24.cz](#) (2a02:4a8:ac24:100:0:0:96:6)

Assessed on: Fri, 09 Oct 2015 02:14:11 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

Velký pomocník je online nástroj [ssllabs.com](#) od Qualys. Známkuje nastavení šifer na vašem HTTPS podobně, jako se známkuje pračky a ledničky v obchodech. Hodnocení je průběžně aktualizováno podle aktuálních znalostí. Jednou za čas se určitě sami otestujte.

Generate Mozilla Ser x

https://mozilla.github.io/server-side-tls/ssl-config-generator/

mozilla

Mozilla SSL Configuration Generator

Apache Modern Server Version
 Nginx Intermediate OpenSSL Version
 HAProxy Old HSTS Enabled
 AWS ELB

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | [link](#)

Oldest compatible clients : Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

```
<VirtualHost *:443>
...
SSLEngine on
SSLCertificateFile      /path/to/signed_certificate
SSLCertificateChainFile /path/to/intermediate_certificate
SSLCertificateKeyFile   /path/to/private/key
SSLCACertificateFile    /path/to/all_ca_certs

# intermediate configuration, tweak to your needs
SSLProtocol              all -SSLv2 -SSLv3
SSLCipherSuite           ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:EC
SSLHonorCipherOrder     on
```

Někdy může být složité na serveru konkrétní šifry správně nastavit. Můžete proto použít tento nástroj, který vhodnou konfiguraci vygeneruje.

OK, mám A. Ted' mohu být v klidu?

Takže když mám na SSL Labs známku „A“ a veškerý HTTP provoz přesměřávám na HTTPS, tak už mi MITM útoky nehrozí?



Bohužel hrozí – problém je v tom úvodním přesměrování, které MITM může zachytit a udržet vás na nešifrovaném spojení. Říká se tomu SSL Stripping. Když zadáme adresu do prohlížeče, obvykle neuvádíme protokol a prohlížeč tedy použije HTTP. Na HTTPS nás přesměruje až následná odpověď serveru, kterou útočník může zachytit a modifikovat.

HSTS

Řešením je HTTP Strict Transport Security, které vašemu prohlížeči říká, že má web načítat rovnou po HTTPS a na HTTP se vůbec nedotazovat. Tuto informaci si prohlížeč zapamatuje ihned po první návštěvě takto zabezpečeného webu. Pokud nastavíte, aby si to prohlížeče pamatovaly alespoň půl roku, SSL Labs vás odmění známkou „A+“.

Fajn, tak jdeme na A+

A jak tedy HSTS nastavit?



```
Strict-Transport-Security "max-age=15768000; IncludeSubdomains; Preload"
```

Pokud budete googlovat, jak HSTS nastavit, najdete pravděpodobně něco podobného tomuto. Ale velký pozor, takhle to nedělejte!

Evidencia

- F1- Žiad. o štatút užívateľa [T]
- F7 - Zmena údajov užív. [T]
- F10 - Výpoveď Rámcovej zmluvy [T]

Evidencia registrátorov

- F2 - Žiad. o štatút registrátora [T]
- Žiad. o nové heslo [T]

Doménové záznamy

- F6 - Zmena Držiteľa [T]
- F8 - Zruš. Registrátora z Dom. [T]
- F12 - Výpoveď zmluvy o Doméne [T]

[T] - Ticketová operácia

Aktuálny počet zaregistrovaných SK domén k 09-10-2015 o 12:52
331316

Zaviedli sme ochranu systému SK-NIC pred útokmi na úrovni maximálneho povoleného počtu prihlásení registrátora v reálnom čase. V súčasnosti je nastavený maximálny počet simultánnych prihlásení na počas celého dňa na úroveň 5.

Vážený návštevník,

vítame vás na stránkach SK-NIC, venovaných správe internetovej domény najvyššej úrovne .sk, ktorá je vyhradená pre slovenský internet. Doména .sk vznikla v roku 1993 a jej správou je poverená spoločnosť SK-NIC, a.s. (predtým EuroWeb Slovakia a.s. a EUnet Slovakia s.r.o.).

Novinky

1.8.2015 Ukončenie podpory Windows XP

Vážený užívateľia, dovoľujeme si vás informovať, že spoločnosť SK-NIC, a.s. v snahe chrániť svojich užívateľov prechádza od 1. 8. 2015 na vyššiu úroveň bezpečnosti, čo spôsobí že už nebude podporované používanie systémov SK-NIC, a.s. z počítačov s operačným systémom Windows XP, prípadne starším, a to najmä vo vzťahu k protokolu HTTPS (SSLv3 a TLSv1). Spoločnosť Microsoft ukončila podporu operačného systému Windows XP už pred viac ako rokom a prestáva opravovať novo identifikované bezpečnostné chyby, čo znamená významné bezpečnostné riziko. Užívateľom preto odporúčame používať novšie operačné systémy.

Ak si chcete otestovať, či vám bude zabezpečené spojenie fungovať správne, na adrese <https://www-ssl-upgrade.sk-nic.sk> sme pre vás pripravili testovaciu stránku. Zároveň upozorňujeme, že testovacia stránka aktuálne používa vlastný certifikát, vzhľadom na čo sa na začiatku objaví upozornenie o nedôveryhodnosti, preto je potrebné odkliknúť časť „rozumiem možným rizikám... / pokračovať v používaní...“ a pokračovať ďalej. Za porozumenie ďakujeme!

Např. v SK-NIC si chtěli také SSL lépe nastavit a zřejmě také googlovali. Nasadili pak HSTS včetně IncludeSubdomains, tedy na všech subdoménách pod sk-nic.sk.



Vaše připojení není soukromé

Útočníci se mohou pokusit ukrást vaše údaje na webu **www-ssl-upgrade.sk-nic.sk** (například hesla, zprávy nebo informace o platebních kartách).

NET::ERR_CERT_AUTHORITY_INVALID

Automaticky Googlu hlásit podrobnosti možných bezpečnostních incidentů. [Zásady ochrany soukromí](#)

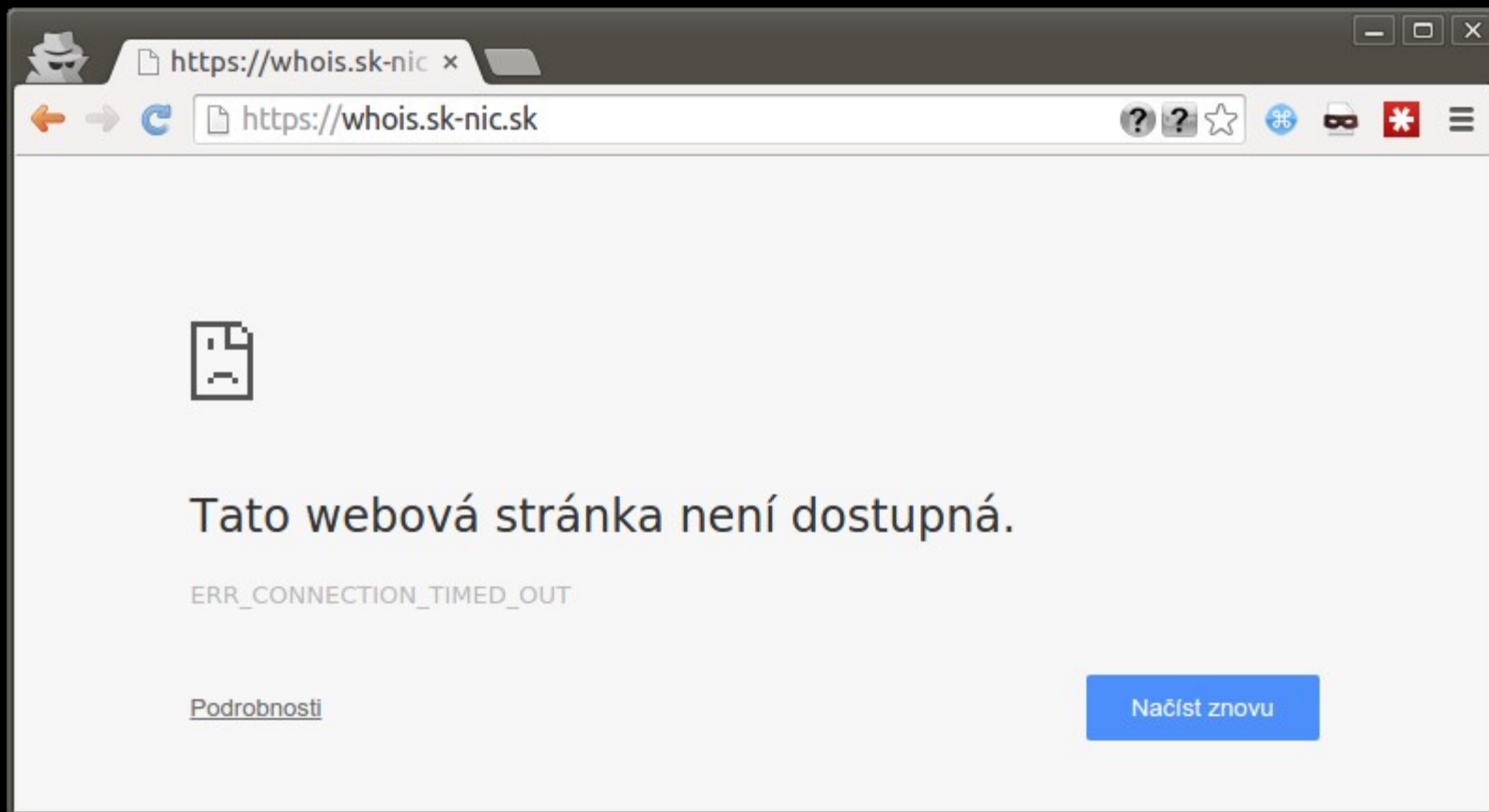
[Skrýt rozšířené](#)

Načíst znovu

Web **www-ssl-upgrade.sk-nic.sk** vaše informace běžně chrání šifrováním. Když se Chrome k webu **www-ssl-upgrade.sk-nic.sk** pokusil připojit tentokrát, web vrátil neobvyklé a nesprávné identifikační údaje. Buď se za web **www-ssl-upgrade.sk-nic.sk** pokouší vydávat nějaký útočník, nebo bylo připojení přerušeno přihlašovací obrazovkou sítě Wi-Fi. Vaše informace jsou i nadále v bezpečí, protože prohlížeč Chrome připojení přerušil dříve, než došlo k odeslání jakýchkoliv dat.

Web **www-ssl-upgrade.sk-nic.sk** nyní nemůžete navštívit, protože používá zabezpečení HSTS. Síťové chyby a útoky jsou obvykle dočasné, tato stránka pravděpodobně později bude fungovat.

Testovací doména s nevalidním certifikátem, kde si lidé měli novou konfiguraci otestovat, se tak stala nedostupnou. Se zapnutým HSTS již není možné hlášení o nevalidním certifikátu přeskočit! Web se tak stává zcela nedostupný, dokud nedodáte validní certifikát.



Služba whois na doméně whois.sk-nic.sk se stala taktéž nedostupnou, protože vůbec na HTTPS neběží. HSTS vás na nezabezpečenou variantu webu nepustí.

Protocols	
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Vzpomínáte, že oznamovali ukončení podpory pro Windows XP? Udělali to tak, že zakázali všechny protokoly kromě nejnovějšího TLS 1.2.

Android 2.3.7	No SNI ²	Protocol or cipher suite mismatch	Fail ³
Android 4.0.4		Protocol or cipher suite mismatch	Fail ³
Android 4.1.1		Protocol or cipher suite mismatch	Fail ³
Android 4.2.2		Protocol or cipher suite mismatch	Fail ³
Android 4.3		Protocol or cipher suite mismatch	Fail ³
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Baidu Jan 2015		Protocol or cipher suite mismatch	Fail ³
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Chrome 43 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 39 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
IE 6 / XP	No FS ¹ No SNI ²	Protocol or cipher suite mismatch	Fail ³
IE 7 / Vista		Protocol or cipher suite mismatch	Fail ³
IE 8 / XP	No FS ¹ No SNI ²	Protocol or cipher suite mismatch	Fail ³
IE 8-10 / Win 7 R		Protocol or cipher suite mismatch	Fail ³
IE 11 / Win 7 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
IE 10 / Win Phone 8.0		Protocol or cipher suite mismatch	Fail ³
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Edge 12 / Win 10 (Build 10130) R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Java 6u45	No SNI ²	Protocol or cipher suite mismatch	Fail ³
Java 7u25		Protocol or cipher suite mismatch	Fail ³

Výsledkem je celá plejáda klientů, kteří se na tento web už nepodívají.

```
Strict-Transport-Security "max-age=15768000; IncludeSubdomains; Preload"
```

Z SK-NIC si tedy příklad neberte. Jak nastavit šifry poradí dříve zmíněný Mozilla SSL Configuration Generator. A u HSTS začněte bez dlouhého max-age, bez IncludeSubdomains a bez Preload.

```
Strict-Transport-Security "max-age=900"
```

Začněte např. s 15 minutovým max-age, který lze v tomto čase zase vypnout, pokud se objeví nečekané potíže. Řešit budete muset zejména tzv. mixed-content, kdy stránka načítaná po HTTPS obsahuje prvky načítané po HTTP.

```
Strict-Transport-Security "max-age=86400"
```

Po odladění můžete čas zvýšit např. na 24 hodin a čekat, jestli vám někdo neohlásí problém, kvůli kterému byste museli HSTS ještě vypínat.

```
Strict-Transport-Security "max-age=604800"
```

Pak zvyšte dejme tomu na týden a čekejte i několik týdnů, jestli nepřijde report chyby. Někdy to může trvat, než se problém od uživatelů dostane až k vám.

```
Strict-Transport-Security "max-age=15768000"
```

A když už to běží třeba měsíc bez potíží, nastavte teprve ten požadovaný půlrok a radujte se z „A+“ známky na SSL Labs.

IncludeSubdomains a Preload používajte až tehdy, když víte přesně, co děláte a že jste nezapomněli na žádnou subdoménu, které se to může týkat.

**A když přejdou na HTTPS,
nepropadnou se ve vyhledávacích?**

Google | Webmaster Central Blog

Official news on crawling and indexing sites for the Google index

HTTPS as a ranking signal

Google vás za takový přechod naopak odmění mírným zvýhodněním webu. Ale spíše to ani nepoznáte – hlavním SEO signálem je stále obsah webu.



[Home](#)
[Chromium](#)
[Chromium OS](#)

Quick links

[Report bugs](#)
[Discuss](#)
[Sitemap](#)

Other sites

[Chromium Blog](#)
[Google Chrome Extensions](#)
[Google Chrome Frame](#)

Except as otherwise [noted](#), the content of this page is licensed under a [Creative Commons Attribution 2.5 license](#), and examples are licensed under the [BSD License](#).

[Chromium](#) > [Chromium Security](#) >

Deprecating Powerful Features on Insecure Origins

We (Chrome Security) originally sent this out to various browser development mailing lists. See the original [intent-to-deprecate email on blink-dev](#). This is based on the original idea to [prefer secure origins for powerful new features](#).

This is a living document — as we learn more, we'll probably need to change this page.

Proposal

We want to start applying the concepts in <https://w3c.github.io/webappsec/specs/powerfulfeatures/> to features that have already shipped and which do not meet the (new, not present at the time) requirements. We want to start by requiring secure origins for these existing features:

- Device motion / orientation
- EME
- Fullscreen
- Geolocation
- getUserMedia()

As with gradually [marking HTTP as non-secure](#), we expect to gradually migrate these features to secure-only, based on thresholds of usage, starting with lowest usage and moving towards higher. We also expect to gradually indicate in the UX that the features are deprecated for non-secure origins.

Kromě vyhledávání je dobré vědět, že bez HTTPS nebudete moci využívat některé služby Googlu ve své aplikaci, např. geolokaci. Seznam takových služeb se bude rozšiřovat.



Seznam Vyhledávání
@hledani_seznam



Sledovat

Naše prohlášení o aktuálním stavu HTTPS stránek v Seznam.cz vyhledávání si můžete přečíst zde:

fulltext.sblog.cz/2015/10/06/325...

Seznam nedávno vydal prohlášení, že k webům na HTTP a HTTPS se již chová naprosto stejně a přechod z HTTP na HTTPS má stejný vliv, jako přechod na jinou doménu pomocí přesměrování. K dočasnému propadu tedy dojít může, ale pokud nejste životně závislí na výsledcích vyhledávání na Seznamu, s přechodem na ně nečekejte. U nových webů už není co řešit.

**OK a kromě bezpečnosti má
HTTPS nějaké výhody?**

HTTP/2

Na HTTPS můžete využívat nový HTTP/2 protokol, který používá několik technik významně zrychlujících načítání stránek a to zejména na mobilech s pomalým připojením. Ačkoliv lze teoreticky HTTP/2 používat i nešifrovaně, v praxi to nikdo nedělá a prohlížeče i servery používají nový protokol jen na HTTPS.

HTTP vs HTTPS Test

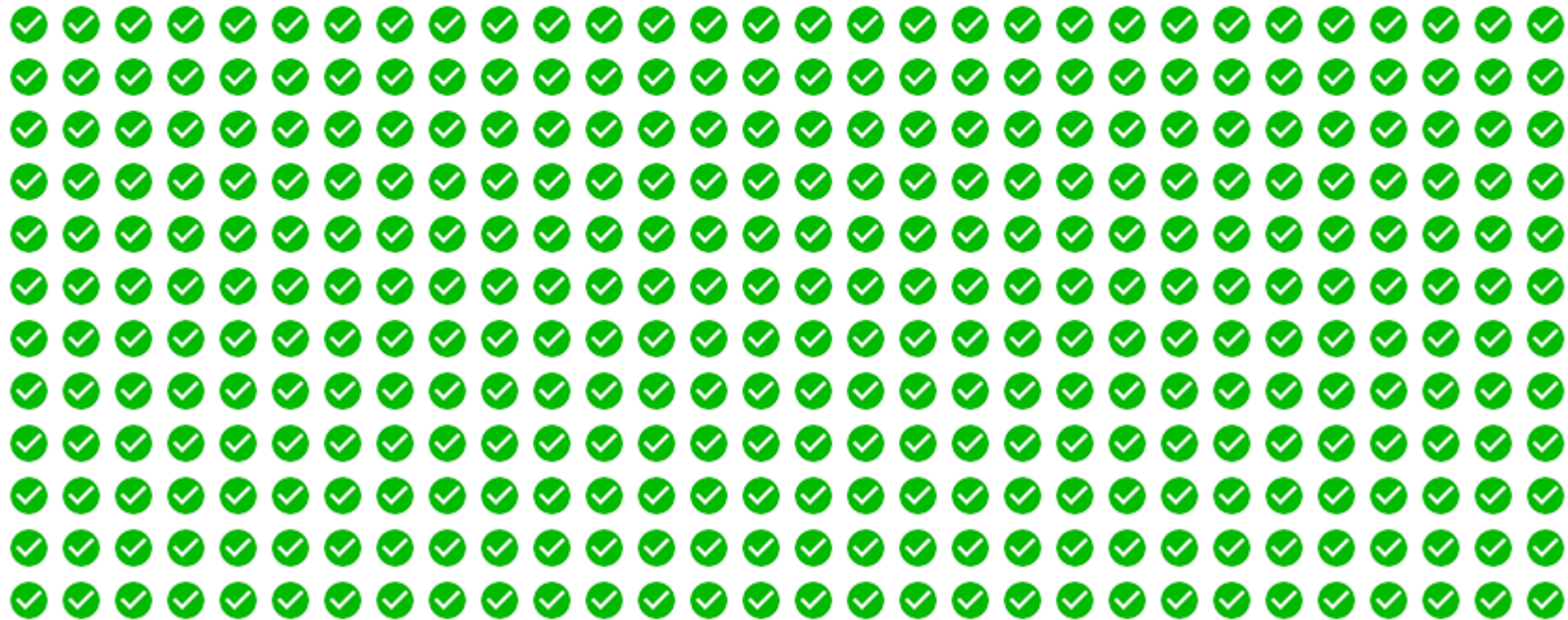
HTTP **HTTPS**

Encrypted Websites Protect Our Privacy and are Significantly Faster¹

Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (2.04 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

9.364 s

Done! Please try HTTPS.



Takhle vypadá načítání mnoha malých obrázků po stávajícím HTTP/1.1

HTTP vs HTTPS Test

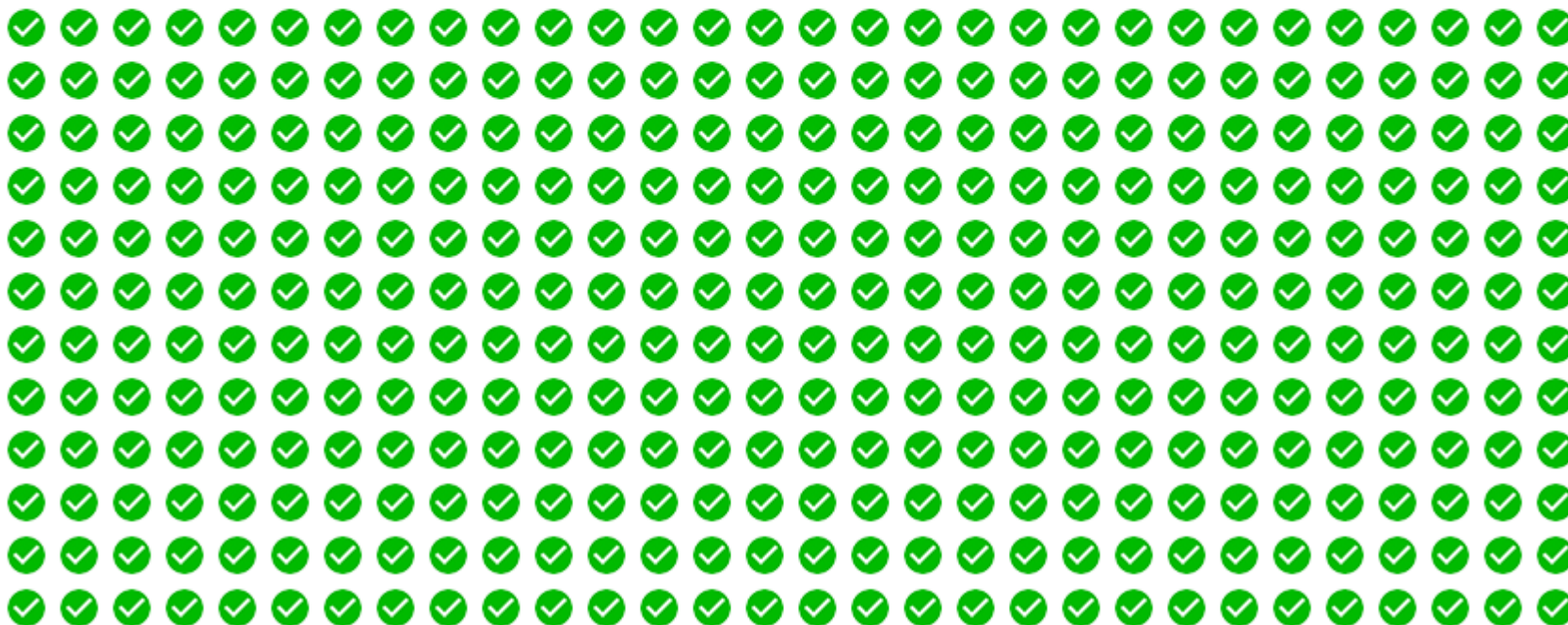
HTTP HTTPS

Encrypted Websites Protect Our Privacy and are Significantly Faster¹

Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (2.04 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

1.630 s

83% faster than HTTP



A takhle po HTTPS s HTTP/2.

A on už to někdo podporuje?

active 24

nginx news



2015-09-22 [nginx-1.9.5](#) mainline version has been released, featuring experimental [HTTP/2 module](#).

Prohlížeče to podporují už dávno, servery donedávna jen u velkých providerů jako Google či Twitter. Od konce září je ale podpora v serveru Nginx. Do Apache existuje zatím neoficiální modul.



Report Details

Network Server on 443

Nice, this host has a network service listening on port 443. SPDY works over [SSL/TLS](#) which usually listens on port 443.

SSL/TLS Detected

Good, this host is speaking [SSL/TLS](#). SPDY piggybacks on top of SSL/TLS, so a website needs SSL/TLS to use SPDY.

Valid X.509 Certificate

This website is responding with a valid [X.509 certificate](#). X.509 certificate errors can cause the browser to display warning messages and to stop speaking with the website, so using a valid certificate is an essential step to supporting SPDY.

ServerHello Contains NPN Extension

Nice, this server including the [NPN Extension](#) during the SSL/TLS handshake. The NPN Extension is an additional part of the [SSL/TLS ServerHello message](#) which allows the web server to tell browser it supports additional protocols, like SPDY.

Success! SPDY is Enabled!

Hurray, this website is using SPDY! The following protocols are supported:

- spdy/3.1
- http/1.1

HTTP Fallback Detected

This website is using SPDY, but it also supports traditional HTTP over SSL. This ensures that older web browsers can still access this site using HTTP

HTTP Redirects to SPDY

Pretty Sexy! Accessing this website via HTTP automatically redirects the user to access the website via SSL/TLS and SPDY. This means all of website's visitors that can browse the site with SPDY, do browse the site using SPDY.

Strict-Transport-Security Supported

Excellent! This website is using HSTS, also known as Strict Transport Security. This tells the browser to always use SSL when talking to this website, allows more of your visitors the opportunity to both be secure and to use SPDY. The server is sending the header `Strict-Transport-Security: max-age=15552000` which tells the web browser to always use SSL to access this website for the next **180** days.

Takto jsme se chlubili podporu SPDY na konferenci
Internet a Technologie 2015.



www.active24.cz Does Not Support SPDY

Report Details

Network Server on 443

Nice, this host has a network service listening on port 443! SPDY works over [SSL/TLS](#) which usually listens on port 443.

TLS v1.2 Connection Detected

Good, this host is speaking [SSL/TLS](#), specifically TLS v1.2. SPDY piggybacks on top of SSL/TLS, so a website needs SSL/TLS to use SPDY.

Valid X.509 Certificate

This website is responding with a valid [X.509 certificate](#). X.509 certificate errors can cause the browser to display warning messages and to stop speaking with the website, so using a valid certificate is an essential step to supporting SPDY.

ServerHello Contains NPN Extension

Nice, this server including the [NPN Extension](#) during the SSL/TLS handshake. The NPN Extension is an additional part of the [SSL/TLS ServerHello message](#) which allows the web server to tell browser it supports additional protocols, like SPDY.

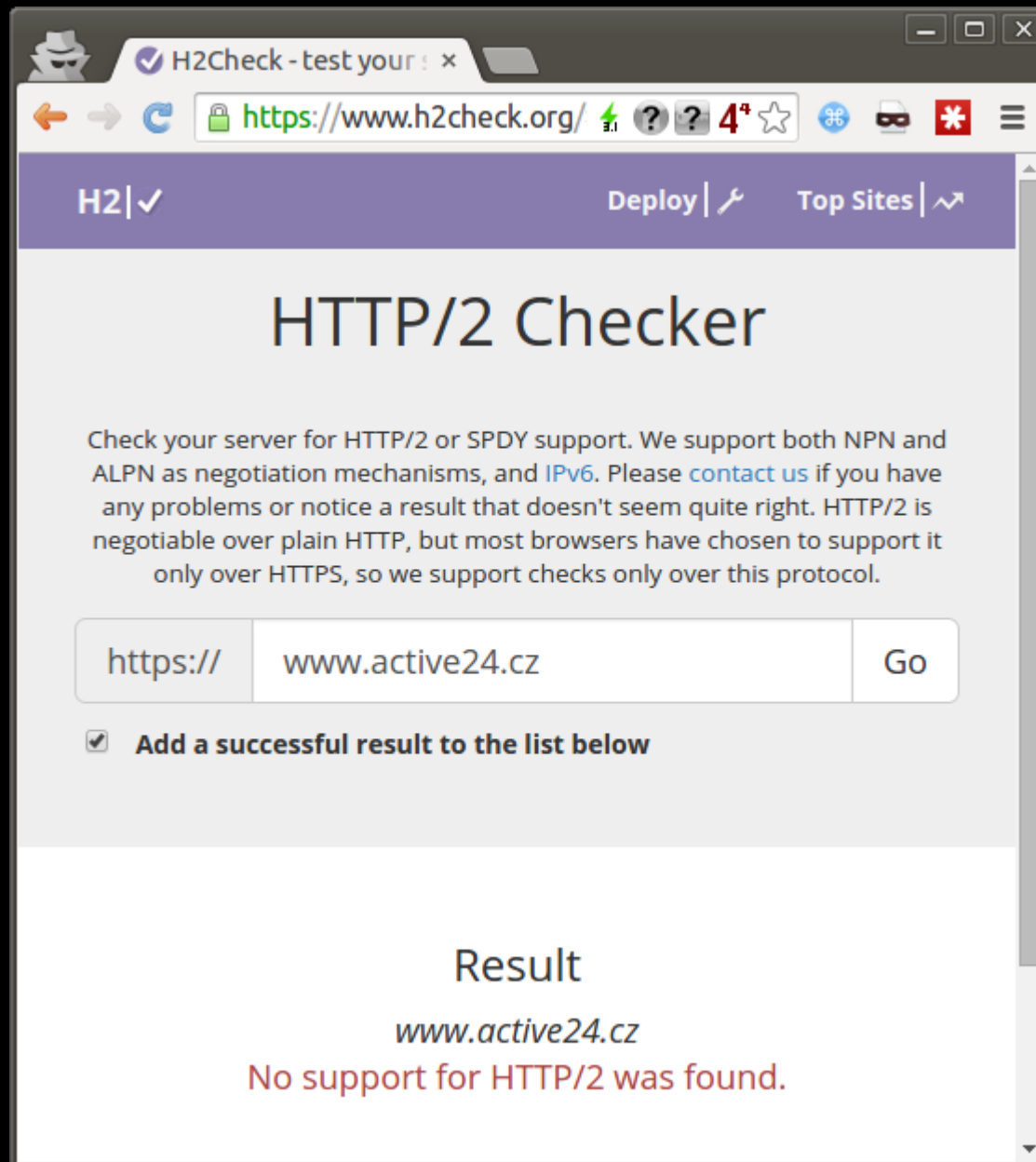
SPDY Protocol Not Enabled!

Seriously? This SSL/TLS server is using the [NPN Extension](#) to tell browsers it supports alternative protocols, but SPDY is not a protocol it supports. The server is not making SPDY an option. Since all the pieces are in place, hopefully it will be easy to enable SPDY support with this server.

HTTP Redirects to HTTPS

Nice job! Accessing this website via HTTP automatically redirects the user to access the website via SSL/TLS. Even though this website doesn't support SPDY yet, this is a good thing. It forces the website's visitors to use SSL/TLS, which makes it easier to offer SPDY support to all capable browsers at some point in the future.

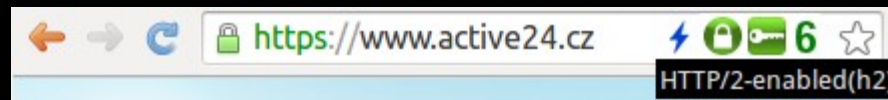
Dnes ten stejný test píše, že SPDY nepodporujeme. Je to vlastně pravda, protože podporujeme již jen HTTP/2.



Horší je, že i HTTP/2 test ukazuje, že tento protokol nepodporujeme. To ale pravda není. Test jen bohužel nerozpozná poslední oficiální revizi tohoto protokolu, ale jen ty starší. Snad to brzy opraví.

```
root@home:~# openssl s_client -nextprotoneg "" -connect active24.cz:443
CONNECTED(00000003)
Protocols advertised by server: h2, http/1.1
3073554056:error:140920E3:SSL routines:SSL3_GET_SERVER_HELLO:parse tlsext:s3_clnt.c:1060:
```

Podporu HTTP/2 u nás tak můžete poznat např. takto pomocí OpenSSL klienta.



Nebo pomocí rozšíření „HTTP/2 and SPDY indicator“ v prohlížeči.

Protocol Details	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Next Protocol Negotiation (NPN)	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=15552000
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

A nebo mnohokrát zmiňovaným SSL Labs testem.

Kolik mě to bude stát?

Bohužel záleží na tom, u koho budete HTTPS resp. HTTP/2 provozovat. Ve většině webhostingových společností je HTTPS stále příplatková služba.

The logo for 'active 24' is located in the bottom right corner. It consists of a red, stylized shape resembling a triangle or a drop, with the text 'active 24' written in white lowercase letters inside it.

active 24






- **HTTPS na všech webech by default**
- **instalace a provoz SSL zcela zdarma**
- **samoobslužná instalace certifikátů**
- **podpora SPDY a následně HTTP/2.0**
- **podpora SSL na IPv6**
- **SSL terminace na reverzní proxy NGINX**

V ACTIVE 24 věříme, že HTTPS má být zdarma dostupné všem v rámci základní služby a ne za příplatek jako opt-in služba. Toto jsme slibovali na konferenci Internet a Technologie 2015.



ACTIVE 24 PLNÍ SLIB A NASAZUJE HTTPS VŠEM ZÁKAZNÍKŮM

A co jsme slíbili, to také plníme. Každý web na našem Linux hostingu má HTTPS rovnou aktivní a to včetně HTTP/2 i na IPv6.

Údaje o serveru					
Doména:	[redacted]				
Alternativní adresa: 	[redacted]				
Operační systém:	Linux				
Hosting:	MULTIHOSTING SUBSERVER				
Umístění:	Expert-4334				nastavení
IP adresa:	81.95.96.166				
IPv6 adresa:	2a02:4a8:ac24:108::96:166				
Aliasy:	----				nastavení
Aliasy včetně e-mailových schránek:	----				
Statistiky spolehlivosti					vstoupit
Informace o službách					
SSL/TLS certifikát	RapidSSL SHA256 CA - G3	expiruje 8.7.2016	Zobrazit	Nahradit	Objednat
Verze PHP	7.0.0RC4 				nastavení
Úroveň PHP	Premium				
Statistiky AWStats					vstoupit
CGI skripty	Ano 				
CRON-periodické spouštění skriptů	neomezeno				nastavení
Vlastní chybové logy	vypnuto 				zapnout
Editace souboru htaccess					nastavení
Automatické vytváření domén 3. řádu	vypnuto 				zapnout

Certifikáty si může zákazník sám aktualizovat dle potřeby přes naše zákaznické centrum. Buď si u nás CRT i koupí, nebo jen vygeneruje CSR a nebo uploaduje vlastní certifikát i s klíčem. Na takovém webu lze rovnou provozovat i poslední PHP 7.0.0 RC4 (default zůstává 5.6).



StartSSL™ Free (Class 1)
128/256-bit Encryption, **1 Year** Validity
Legitimate SSL/TLS + S.MIME Certificates
No Charge, Unlimited + 100 % Free

Validní certifikát lze dnes získat pro nekomerční účely zcela zdarma u Start SSL certifikační autority.



Nebo si počkejte na Let's Encrypt, kde už to bude zdarma pro všechny. Pokud se tyto certifikáty v praxi osvědčí, zákazníkům je rovnou zprostředkujeme.

A co když HTTPS i přesto všechno nechci?

Můžeme o tom diskutovat, můžeme s tím i nesouhlasit, ale to je tak všechno, co se proti tomu dá dělat...

Přechod z HTTP na HTTPS je realita, které se děje právě teď. Má to své mouchy, které je potřeba řešit, ale přijměte to jako fakt.

Děkuji za pozornost!

www.active24.cz

@active24cz

@tomashala

