SSL na hostingu po HeartBleed, POODLE, Snowdenovi a dalších kalamitách

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

28. května 2015

Internet a Technologie 15

06/2013


PRISM

03/2014

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.

04/2014

Support for Windows XP has ended :

0 Days : 0 Hours : 0 Minutes : 0 Seconds

04/2014

08/2014

Google | Webmaster Central Blog

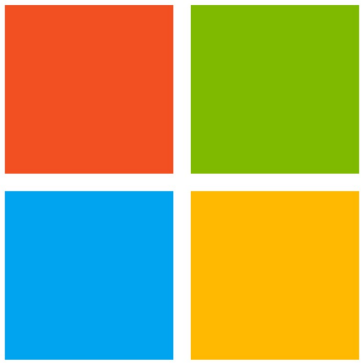
Official news on crawling and indexing sites for the Google index

HTTPS as a ranking signal

10/2014

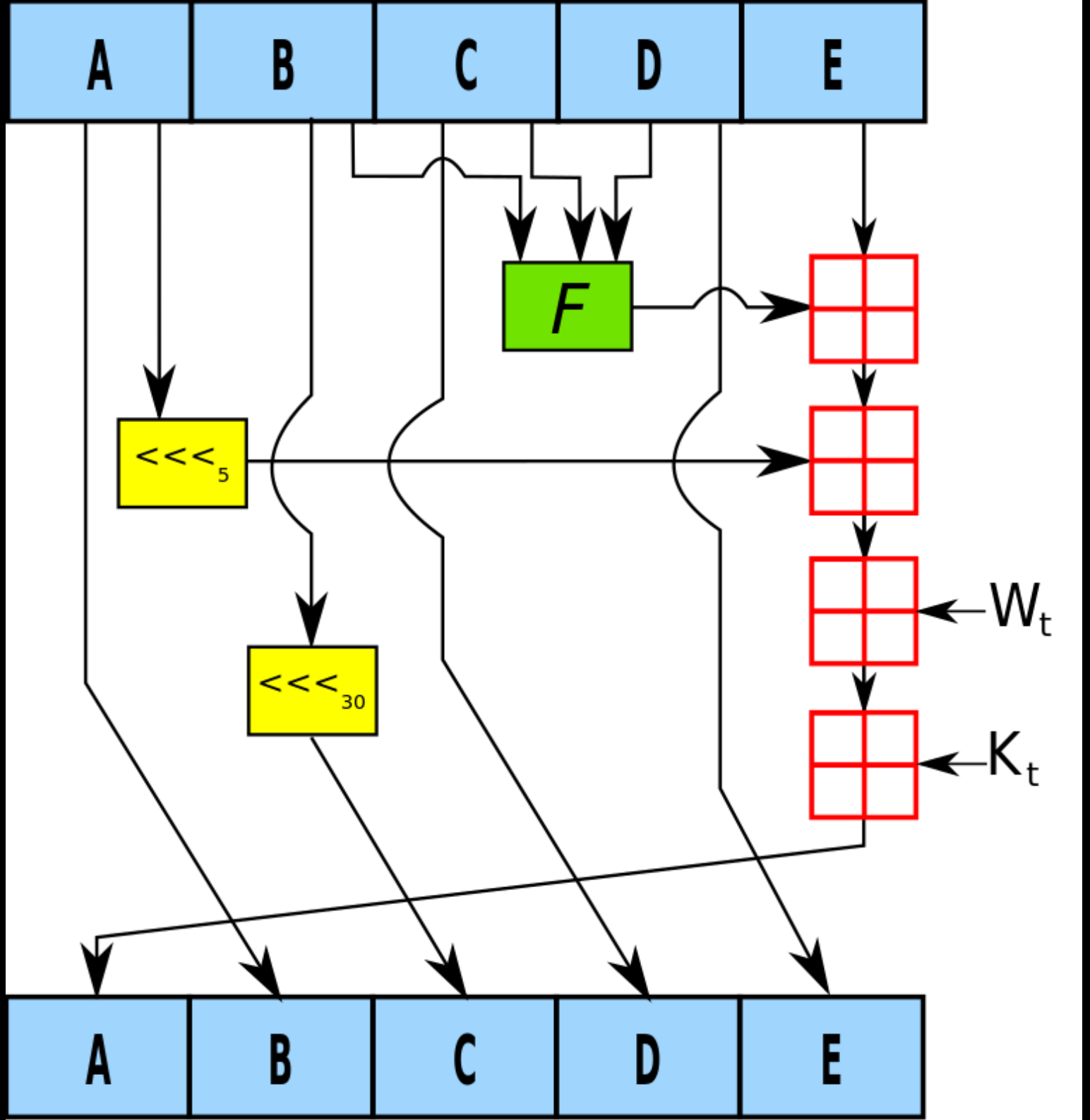

Vulnerable!
Not vulnerable!

11/2014



SChannel

11/2014

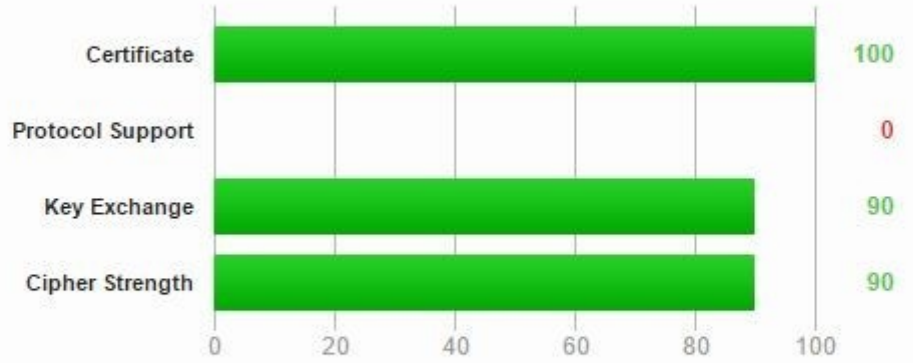

A
B
C
D
E
F
<<<5
<<<30
Wt
Kt
A
B
C
D
E

12/2014

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

03/2015

Tracking the FREAK Attack

Warning! Your browser is vulnerable to the FREAK attack. It can be tricked into using weak encryption if you visit a vulnerable website. We encourage you to update your browser right away.

On Tuesday, March 3, 2015, researchers announced a new SSL/TLS vulnerability called the FREAK attack. It allows an attacker to intercept HTTPS connections between vulnerable clients and servers and force them to use weakened encryption, which the attacker can break to steal or manipulate sensitive data. This site is dedicated to tracking the impact of the attack and helping users test whether they're vulnerable.

05/2015

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:

05/2015

Overall Rating

No support for TLS 1.2, which is the only secure protocol version. MORE »

dnes


014
days since last
logo-branded
vulnerability

Co děláme v ACTIVE 24

- optimalizace konfigurace šifer dle SSL Labs
- pravidelný scan celého našeho IP rozsahu
- rozšiřování HTTPS
- nasazování HSTS
- nasazování SPDY
- testování DANE a Public Key Pinning
- podpora TLSA / SSHFP záznamů

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > active24.cz

SSL Report: active24.cz (81.95.96.6)

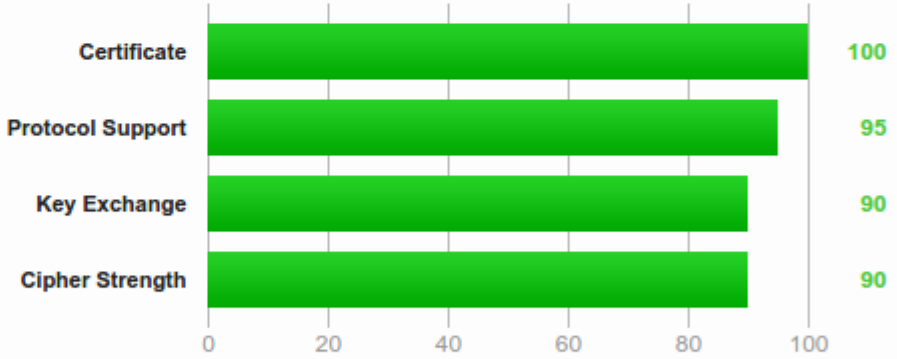
Assessed on: Wed, 27 May 2015 21:14:03 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A+



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 »

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > centrum.active24.cz

SSL Report: centrum.active24.cz (81.95.96.20)

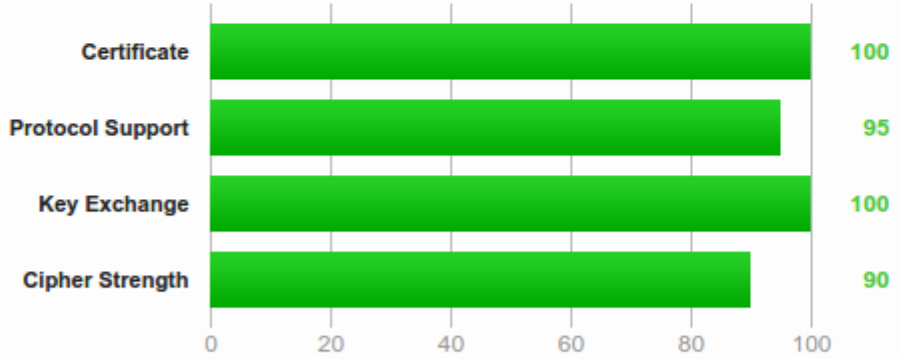
Assessed on: Wed, 27 May 2015 21:37:49 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A+



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 »


https://www.active24.cz
6
www.active24.cz
2a02:4a8:ac24:100::96:6
https://www.active24.cz
Certifikát odpovídá TLSA
Certifikát vzdáleného serveru pro toto doménové jméno byl ověřen protokolem DANE. Certifikát odpovídá záznamu TLSA, který je zabezpečen technologií DNSSEC.
www.active24.cz
Zabezpečeno DNSSEC
Doménové jméno www.active24.cz je korektně zabezpečeno DNSSEC technologií.

www.active24.cz Supports 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.

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 Entension 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 Supporteded
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.

V průběhu června můžete očekávat

- 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

WANTED

- Java EE Junior programátor
- Server administrátor UNIX
- Server administrátor LINUX

active 24

Děkuji za pozornost!

www.active24.cz

twitter.com/active24cz

twitter.com/tomashala