Informace o testu	
Zadané URL serveru:	vutbr.cz
Datum a čas testování:	2021-05-20 10:32:07

Legenda			
Dobře zabezpečený	A+ (100-95)	Částečně zabezpečený	B (79-50)
Zabezpečený	A (94-80)	Zranitelný	C (49-0)

Informace o certifikátu	
Subjekt	C = CZ
	L = Brno-st\C5\99ed
	O = Vysok\C3\A9 u\C4\8Den\C3\AD technick\C3\A9 v Brn\C4\9B
	CN = www.vutbr.cz
Vydavatel	C = NL
	O = GEANT Vereniging
	CN = GEANT OV RSA CA 4
Secure Renegotiation	Bezpečné znovu vyjednávání podporuje
Komprese	NONE (žádná)
Veřejný klíč	RSA 2048 bitů
Podpis	sha384WithRSAEncryption
Platnost od	2021-04-26 00:00:00
Platnost do	2022-04-26 23:59:59
Certifikát je platný	

IP adresy
vutbr.cz (147.229.2.90)
Žádné alternativní adresy

Známka	Skóre serveru
C	42

Porty
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp filtered domain
80/tcp open http
113/tcp filtered ident
443/tcp open https
3389/tcp filtered ms-wbt-server

Podpora HSTS
Ne

Podporované protokoly
TLSv1.2
TLSv1.1
TLSv1.0

Informace o serveru
whois-ip: Record found at whois.ripe.net
inetnum: 147.229.0.0 - 147.229.254.255
netname: VUTBRNET
descr: Brno University of Technology
country: CZ
role: Brno University of Technology - Backbone Admins
email: admin@cis.vutbr.cz

Zranitelnosti	Doporučení
HTTP	Server má povolený nezabezpečený port 80. Hrozí potenciální odposlech spojení. Jak přesměrovat na HTTPS (Apache)
HSTS	Nedetekováno - potenciální útok MITM. Konfigurace HSTS
LUCKY13	Byl použit mód CBC při šifrování. CVE-2013-0169 Detail (NIST)
SHA1	Byl použit slabý hash SHA1. Prolomený SHA1 (NIST)
Výměna klíče přes RSA	Výměna klíče proběhla pomocí RSA algoritmu. Doporučení NIST pro TLS
BEAST Útok	Byly použitý protokoly TLS 1.0 a starší. Doporučení NIST pro TLS

OpenSSL 1.1.1d 10 Sep 2019 - Cipher suits (IANA)	
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_GCM_SHA384
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA