Informace o testu	
Zadané URL serveru:	czc.cz
Datum a čas testování:	2021-05-20 17:42:33

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

Informace o certifikátu	
Subjekt	CN = *.czc.cz
Vydavatel	C = US
	O = DigiCert Inc
	CN = RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
Secure Renegotiation	Bezpečné znovu vyjednávání nepodporuje
Komprese	NONE (žádná)
Veřejný klíč	RSA 2048 bitů
Podpis	sha256WithRSAEncryption
Platnost od	2020-12-03 00:00:00
Platnost do	2022-01-03 23:59:59
Certifikát je platný	

IP adresy
czc.cz (82.99.173.171)
82.99.173.173

Známka	Skóre serveru
A	92

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

Podpora HSTS
Ano

Podporované protokoly
TLSv1.3
TLSv1.2

Informace o serveru
whois-ip: Record found at whois.ripe.net
inetnum: 82.99.173.0 - 82.99.173.255
netname: BLUETONE
descr: Server housing
country: CZ
role: CRA Hostmasters
email: ripe@bluetone.cz

Zranitelnosti	Doporučení
HTTP	Server má povolený nezabezpečený port 80. Hrozí potenciální odposlech spojení. Jak přesměrovat na HTTPS (Apache)
Renegotiation	Server nepodporuje bezpečné opětovné vyjednávání. Informace
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

OpenSSL 1.1.1d 10 Sep 2019 - Cipher suits (IANA)	
TLSv1.3	TLS_AES_256_GCM_SHA384
	TLS_CHACHA20_POLY1305_SHA256
	TLS_AES_128_GCM_SHA256
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	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