Informace o testu	
Zadané URL serveru:	webserver-actinver-prd.lfr.cloud
Datum a čas testování:	2021-05-20 17:32:31

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

Informace o certifikátu	
Subjekt	C = US
	postalCode = 91765
	ST = California
	L = Diamond Bar
	street = 1400 Montefino Ave.
	O = "Liferay, Inc."
	CN = liferay.cloud
Vydavatel	C = GB
	ST = Greater Manchester
	L = Salford
	O = Sectigo Limited
	CN = Sectigo RSA Organization Validation Secure Server CA
Secure Renegotiation	Bezpečné znovu vyjednávání nepodporuje
Komprese	NONE (žádná)
Veřejný klíč	RSA 2048 bitů
Podpis	sha256WithRSAEncryption
Platnost od	2020-05-20 00:00:00
Platnost do	2021-10-24 23:59:59
Certifikát je platný	

IP adresy
webserver-actinver-prd.lfr.cloud (35.186.243.200)
Žádné alternativní adresy

Známka	Skóre serveru
A	82

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 open ms-wbt-server

Podpora HSTS
Ano

Podporované protokoly
TLSv1.3
TLSv1.2

Informace o serveru
whois-ip: Record found at whois.arin.net
netrange: 35.184.0.0 - 35.191.255.255
netname: GOOGLE-CLOUD
orgname: Google LLC
orgid: GOOGL-2
country: US stateprov: CA
orgtechname: Google LLC
orgtechemail: arin-contact@google.com

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_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Zranitelnosti	Doporučení
HTTP	Server má povolený nezabezpečený port 80. Hrozí potenciální odposlech spojení. Jak přesměrovat na HTTPS (Apache)
3389	Server má otevřený port 3389 (RDP). Otevřený přístup ke vzdálené ploše. Doporučeno port zakázat nebo nastavit jiný pro vzdálený přístup. Informace
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)