

Forum:[Hack Forums](#)

Thread: [TLS 1.0 Vulnerability](#)

IvanMolBayd - March 18, 2025, 8:16 am

I have heard about this High TLS 1.0 Vulnerability when scanning for vulnerabilities on a website of mine (bellow is the desription the tool gave me of the vulnerability) , it seemed to be severe and i would be realy apreciative if someone could tell me about how an attacker may use it (im fairly new to this)

The SSL server (port: 443) encrypts traffic using TLSv1.0.

Thanks <3

DramaKing - March 19, 2025, 11:26 am

(Mar 18, 2025 08:16 AM)IvanMolBayd Wrote: [\[CITE\]](#) I have heard about this High TLS 1.0 Vulnerability when scanning for vulnerabilities on a website of mine (bellow is the desription the tool gave me of the vulnerability) , it seemed to be severe and i would be realy apreciative if someone could tell me about how an attacker may use it (im fairly new to this)

The SSL server (port: 443) encrypts traffic using TLSv1.0.

Thanks <3

TLS 1.0 is, of course, bad. It was superseded by TLS 1.1, which was defined by RFC 4346 all the way back in April 2006. You would pretty much need to create your own implementation of TLS or go through some software archive. Microsoft disabled v1.0 and 1.1 in Windows 11 starting in 2023.

A search on Shodan shows that there are nearly 2 million servers running TLS 1.0 and not 1.2 with the largest number located in Venezuela. Huawei Home Gateway represents the largest number of services.