

Forum:[Hack Forums](#)

Thread: [Self-Signed SSL Certificates.](#)

hack3rcon - July 2, 2019, 2:19 pm

Hello.

Is Self-Signed SSL Certificate secure? What is the difference between Self-Signed SSL Certificates and SSL Certificates that provide by companies like Comodo SSL, DigiCert, GoDaddy and...?

Thanks.

Discord - July 2, 2019, 2:23 pm

Unlike CA issued certificates, self-signed certificates are free of charge. ... While self-signed SSL Certificates also encrypt customers' log in and other personal account credentials, they prompt most web servers to display a security alert because the certificate was not verified by a trusted Certificate Authority

SuckySucky - July 2, 2019, 5:14 pm

Take a look at lets encrypt. Signed SSL certifications that are free of charge and introduced wildcard certificates a few months back.

hack3rcon - July 3, 2019, 2:12 am

(Jul 2, 2019 02:23 PM)Discord Wrote: [\[CITE\]](#) Unlike CA issued certificates, self-signed certificates are free of charge. ... While self-signed SSL Certificates also encrypt customers' log in and other personal account credentials, they prompt most web servers to display a security alert because the certificate was not verified by a trusted Certificate AuthorityThus, Self-Signed SSL Certificates are secure and the browsers alerts is because of that the SSL Certificate don't provided by a company that listed in the browser?

atsavurdu - July 14, 2019, 1:49 am

(Jul 2, 2019 05:14 PM)SuckySucky Wrote: [\[CITE\]](#) Take a look at lets encrypt. Signed SSL certifications that are free of charge and introduced wildcard certificates a few months back. Exactly. If you choose to View Certificate, it will show it was issued from you, on your own machine.

rabbi - July 14, 2019, 1:55 am

(Jul 2, 2019 02:19 PM)hack3rcon Wrote: [\[CITE\]](#) Hello.

Is Self-Signed SSL Certificate secure? What is the difference between Self-Signed SSL Certificates and SSL Certificates that provide by companies like Comodo SSL, DigiCert, GoDaddy and...?

Thanks.

many self signed certs are either flagged as not secure or dangerous

ASLR - July 15, 2019, 5:47 pm

Self signed certificates are secure provided you use proper ciphers and strong keys. The issue with using self signed certs for a public facing service is that user's browsers will warn that the service is not secure. User's will get into the habit of ignoring the security warnings and then will not notice if a true MITM attack happened (a malicious party intercepts the traffic and the user initiates a TLS connection using the attacker provided certificate). Self signed certificates are safe for use internally within organizations. Within an organization, you can distribute your root certificate authority to user devices and servers so that the connecting machines trust the self-signed certificate. A security

warning will not be displayed. Self-signed vs vendor issued certificates should be used in different circumstances. They can actually be MORE secure. By using your own certificate authority within your organization you guard against a scenario where an attacker compromises a CA vendor and issues fraudulent certificates which they can use to attack your organization.

ahears - *August 30, 2019, 2:30 am*

I think everyone forgot to answer the question: a Cert from a Certificate Authority (CA) proves you are who you say you are by way of a trusted authority (like Digicert, not Comodo) checking your credentials. A self signed Cert does not have this process, everyone is taking your word for it, and when making a credit card purchase this can be a deal breaker. That said, both certs are secure if they are generated using the latest accepted encryption standards and correctly implemented. This can provide an encrypted communication nobody else can see. No difference between them except credibility and accountability. "Let's Encrypt" certs are fine if you trust the person communicating with you. With a CA issued cert, they would probably get caught and distributing malware or skimming credit cards and threat actors would need to rely on infecting a legit website instead of providing this service for you directly. Without a CA, malware could be distributed directly but over a secure connection. Just because it's encrypted with a Self Signed Cert doesn't make it safe to download!