NIC-CERT/2021-09/232
Dated: 28-09-2021
CVE ID: Multiple
Severity: Critical

Advisory for Let's Encrypt's Certificate Expiry Update

A. Description:

One of the largest providers of HTTPS certificates, Let's Encrypt, will stop using an older root certificate next week which might break devices and cause outages encrypted data transfers.

B. Security Issue:

On 30th September 2021, the root certificate that Let's Encrypt are currently using, the IdentTrust DST Root CA X3 certificate, will expire, breaking a chain of trust that could result in widespread problems during HTTPS communication. So any website or application using this certificate will be unreachable with a warning that accessing the website or application could be dangerous.

Affected Products:

Older and outdated versions of Windows(XP Service Pack 3), MacOS(2016), iOS, Microsoft's IIS webserver and other clients which are still using IdenTrust DST Root CA X3 root certificate and don't trust the new ISRG root certificate are affected by this.

Android: Devices that are running Android operating systems prior to 7.1.1, don't trust the new ISRG Root X1certificate and will be affected by this.

Linux: older versions that use OpenSSL 1.0.2 will be affected by this like RHEL 7 and Ubuntu 16.04.

Most of the modern browsers come with the new ISRG root certificate, Users must manually check if they their systems have new ISRG root certificate installed.

C. Solution:

The device needs to have updated recently enough to get the new ISRG root certificate from Let's Encrypt. Servers need to have an updated certificate chain to serve to clients. If an update is not available, consider below options to solve the issue on OpenSSL 1.0.2 TLS client:

- Remove the IdenTrust DST Root CA X3 root certificate from the trust store and manually install the ISRG Root X1 root certificate (not the cross-signed one).
- If you're using OpenSSL commands like, verify or s_client you can add the -trusted_first flag if possible.
- Have the server serve an alternate certificate chain that goes directly to the ISRG Root X1 (not the cross-signed one)
  https://letsencrypt.org/docs/certificate-compatibility/
- On linux environments, use OpenSSL 1.1.x or later.

Or other temporary solution is to not check the expiration date or extend the expiration date of the certificate.

For APIs:

- All clients of your API must trust ISRG Root X1 (not just DST Root CA X3),
- If clients of your API are using OpenSSL, they must use version 1.1.0 or later.

Android: Install and use latest versions Firefox web browser from playstore on Android versions prior to 7.1.1.

D. Check if you're affected:

On Windows:

- Type "Manage Computer Certificates" in Start Menu search and open it.
- From the left panel expand "Trusted Root Certification Authorities" and Select Certificates
- Look for DST Root CA X3 certificate and check the expiry date of the certificate.
- Also look for ISRG Root X1.

On Linux:

- Open '/etc/ssl/certs/' directory in terminal,
- Look for DST Root CA X3 certificate and
  enter the following command to view certificate info:
  "Openssl x509 -text -noout -in DST_Root_CA_X3.pem"

- Also look for ISRG Root X1 certificate in the same directory

If the expiry date of the DST Root CA X3 certificate its 30 September, and ISRG Root X1 certificate is not present you are affected by this.

E. References:

https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

https://portswigger.net/daily-swig/device-breakage-concerns-persist-days-before-lets-encrypt-root-cert-expiry

https://scotthelme.co.uk/lets-encrypt-old-root-expiration/

https://www.openssl.org/blog/blog/2021/09/13/LetsEncryptRootCertExpire/