Field Notice: FN - 72094 - Secure Unique Device Identifier Expiration Might Impact Certain Functions on IoT Products Running Cisco IOS or Cisco IOS-XE Platforms - Workaround

Updated: April 29, 2021 **Document ID:** FN72094

Bias-Free Langua

Notice

THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS FIELD NOTICE AT ANY TIME.

Revision History

Revision	Publish Date	Comments
1.0	01-Apr-21	Initial Release
1.1	29-Apr-21	Updated the Background Section

Products Affected

Affected Product ID	Comments
CGR1120/K9	
CGR1240/K9	
CGR1240/K9=	
IR807G-LTE-GA-K9	
IR807G-LTE-NA-K9	
IR807G-LTE-VZ-K9	
IR809G-LTE-GA-K9	
IR809G-LTE-NA-K9	
IR809G-LTE-LA-K9	
IR809G-LTE-VZ-K9	
IR829-2LTE-EA-AK9	
IR829-2LTE-EA-BK9	

IR829-2LTE-EA-EK9	
IR829B-2LTE-EA-AK9	
IR829B-2LTE-EA-BK9	
IR829B-2LTE-EA-EK9	
IR829B-2LTE-EA-RK9	
IR829B-LTE-EA-AK9	
IR829B-LTE-EA-BK9	
IR829B-LTE-EA-EK9	
IR829B-LTE-EA-RK9	
IR829GW-LTE-GA-CK9	
IR829GW-LTE-GA-EK9	
IR829GW-LTE-GA-SK9	
IR829GW-LTE-GA-ZK9	
IR829GW-LTE-LA-DK9	
IR829GW-LTE-LA-FK9	
IR829GW-LTE-LA-HK9	
IR829GW-LTE-LA-KK9	
IR829GW-LTE-LA-LK9	
IR829GW-LTE-LA-NK9	
IR829GW-LTE-LA-QK9	
IR829GW-LTE-LA-SK9	
IR829GW-LTE-LA-TK9	
IR829GW-LTE-LA-ZK9	
IR829GW-LTE-NA-AK9	
IR829GW-LTE-VZ-AK9	
IR829M-2LTE-EA-AK9	
IR829M-2LTE-EA-BK9	
IR829M-2LTE-EA-EK9	
IR829M-2LTE-EA-RK9	
IR829M-LTE-EA-AK9	
IR829M-LTE-EA-BK9	
IR829M-LTE-EA-EK9	

IR829M-LTE-EA-RK9	
IR829M-LTE-EA-ZK9	
CGR-2010/K9	
CGR-2010/K9=	
IE-5000-16S12P	
IE-5000-12S12P-10G	
IE-5000-24-10GE-TM	
IE-4010-16S12P	
IE-4010-16S12P=	
IE-4010-4S24P	
IE-4010-4S24P=	
IE-4000-16GT4G-E	
IE-4000-8T4G-E	
IE-4000-8S4G-E	
IE-4000-8GT8GP4G-E	
IE-4000-8GT4G-E	
IE-4000-8GS4G-E	
IE-4000-4TC4G-E	
IE-4000-4T4P4G-E	
IE-4000-4S8P4G-E	
IE-4000-4GS8GP4G-E	
IE-4000-4GC4GP4G-E	
IE-4000-16T4G-E	
IE-3010-16S-8PC	
IE-3010-16S-8PC-U	
IE-3010-24TC	
IE-3100-24TC	
CGS-2520-16S-8PC	
CGS-2520-16S-8PC=	
CGS-2520-24TC	
CGS-2520-24TC=	
IE-1000-4P2S-LM	

IE-1000-4T1T-LM	
IE-1000-6T2T-LM	
IE-1000-8P2S-LM	
IR829M-LTE-LA-ZK9	
IR829M-2LTE-LA-ZK9	
IR829M-2LTE-LA-EK9	
IR829GW-LTE-SC-BK9	
IR829GW-LTE-SC-K9	
IR829GW-LTE-LA-EK9	
IR829GW-LTE-GA-RK9	
IR829B-LTE-LA-ZK9	
IR829GW-2LTE-EA-BK9	
IR829GW-2LTE-LA-ZK9	
IR829GW-LTE-EA-BK9	
IR829B-2LTE-LA-ZK9	
IR829-2LTE-LA-ZK9	
IR809G-LTE-SC-K9	
IR809G-3G-GA-K9	

Defect Information

Defect ID	Headline
CSCvx28898	SUDI certificate expiration may impact functionality

Problem Description

The Cisco Secure Unique Device Identifier (SUDI) certificate, when registered to a Public Key Infrastructure (PKI) AND used to configure certain functionalities on Cisco IOS and IOS XE, will expire on a limited number of Cisco products (see the Products Affected section). Any service that relies on a SUDI certificate to establish a secure connection might not work after the certificate expires.

Background

SUDI is an X.509v3 certificate which maintains the product identifier and serial number. The identity is implemented at manufacturing and is link

SUDI can be used as an immutable ident

The Cisco SUDI certificate, when registered to a PKI and used to configure certain functionalities on Cisco IOS and Cisco IOS XE, will expire on a limited number of Cisco products either on [the date of manufacture + 10 years] or 2029-05-14, whichever is earlier. Any service which relies on a SUDI certificate to establish a secure connection might NOT work after the certificate expires.

In order to determine the SUDI certification expiration date, enter this command:

```
router>show crypto pki certificates

Certificate

Status: Available

Certificate Serial Number (hex): 051E49D9

Certificate Usage: General Purpose

Issuer:

cn=ACT2 SUDI CA

o=Cisco

Subject:

Name: ISR4331/K9

Serial Number: PID:ISR4331/K9 SN:FDO241617C1

cn=ISR4331/K9

ou=ACT-2 Lite SUDI

o=Cisco

serialNumber=PID:ISR4331/K9 SN:FDO241617C1

Validity Date:

start date: 02:23:17 UTC Apr 20 2020

end date: 20:25:41 UTC May 14 2029

Associated Trustpoints: CISCO_IDEVID_SUDI
```

In order to determine if a SUDI trust point is used, enter this command:

```
Router# show run | i CISCO_IDEVI
```

Various features that might be linked to the SUDI certificate are shown in these sample configurations:

HTTPS

```
ip http secure-trustpoint CISCO_IDEVID_SUDI
ip http client secure-trustpoint CISCO_IDEVID_SUDI
```

SSH Authentication Using Certificates

```
ip ssh server certificate

   profile  server

      trustpoint sign CISCO_IDEVID_SUDI
```

ZTD Using a Certificate Enrollment Profile for Enrollment or Reenrollment

```
crypto pki profile enrollment profile-name

   credential CISCO_IDEVID_SUDI
```

Note: Ignoring the expiration date on the SUDI certificate does NOT weaken the ability to use it to authenticate the identity (AuthN) of a Connected Grid Router (CGR) because this is in sync with IEEE 802.1 AR, which recommends that the initial identity certificates do NOT expire. Since the SUDI certificate can continue to be used for AuthN, it can be the basis of a customer's authorization (AuthZ) to admit any given CGR to their network or to otherwise trust the device.

Problem Symptom

Any services that rely on a trust point configured with an expiring Cisco SUDI certificate will be affected. Some examples are:

- HTTP Server over TLS (HTTPS) - HTTPS will produce an error in the browser which indicates that the certificate is expired.
- SSH Server - Applications that use SUDI certificates to authenticate the SSH session might fail to authenticate.
  Note: This use of SUDI certificates is rare. Username/password authentication and non-SUDI public/private key authentication are not affected.

Workaround/Solution

Customers should use one of these four workaround methods in order to install/use an alternate certificate:

1. Install a certificate from a CA.
2. Use the local Cisco IOS CA server to generate and sign a new certificate.
3. Use OpenSSL to generate a PKCS12 certificate bundle and import the bundle to Cisco IOS.
4. Acquire a certificate from the customer's PKI using Simple Certificate Enrollment Protocol (SCEP).

Notes:

- Introduction of a new certificate on a device might require importing the issuer's certificate on any peer devices on which communication is protected using the new certificate.
- After a new non-SUDI certificate is obtained, the configuration of a feature identified in the Background section must be updated b
  able to use the new certificate.

Workaround 1

Install a certificate from a CA.

In this workaround, a certificate request is generated and displayed by Cisco IOS. The administrator then copies the request and submits it to a third-party CA and retrieves the result.

Note: Use of a CA to sign certificates is a security best-practice. This procedure is provided as a workaround in this field notice. However, it is preferable to continue to use the third-party CA-signed certificate after you apply this workaround, rather than to use a self-signed certificate.

In order to install a certificate from a third-party CA, complete these steps:

1. Create a Certificate Signing Request (CSR).

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment term pem
Router(ca-trustpoint)# subject-name CN=TEST
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair TEST
Router(ca-trustpoint)# exit
Router(config)# crypto pki enroll TEST
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=TEST
% The subject name in the certificate will include: Router.cisco.com
% The serial number in the certificate will be: FTX1234ABCD
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
A Base64 Certificate is displayed here. Copy it, along with the ---BEGIN and
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---
```

2. Submit the CSR to the third-party CA.
Note: The procedure to submit the CSR to a third-party CA and retrieve the resulting certificate varies based on the CA that is used. Consult the documentation of your CA for instructions on how to perform this step.

3. Download the new identity certificate for the router along with the CA certificate.

4. Install the CA certificate on the device.

```
Router# conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# crypto pki auth TEST


Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself


-----BEGIN CERTIFICATE-----

REMOVED

-----END CERTIFICATE-----


Certificate has the following attributes:

   Fingerprint MD5: 79D15A9F C7EB4882 83AC50AC 7B0FC625
```

```
     Fingerprint SHA1: 0A80CC2C 9C779D20 9071E790 B82421DE B47E9006


  % Do you accept this certificate? [yes/no]: yes

  Trustpoint CA certificate accepted.

  % Certificate successfully imported


  Install the identity certificate on the device.

  Router(config)# crypto pki import TEST certificate


  Enter the base 64 encoded certificate.

  End with a blank line or the word "quit" on a line by itself


  -----BEGIN CERTIFICATE-----

  REMOVED

  -----END CERTIFICATE-----


  % Router Certificate successfully imported
```

Workaround 2

Use the local Cisco IOS CA server to generate and sign a new certificate.

Note: The local CA server feature is NOT available on all products.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip http server
Router(config)# crypto pki server IOS-CA
Router(cs-server)# grant auto
Router(cs-server)# database level complete
Router(cs-server)# no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: <password>


Re-enter password: <password>
% Generating 1024 bit RSA keys,
[OK] (elapsed time was 1 seconds)


% Certificate Server enabled.
```

```
Router# show crypto pki server IOS-CA Certificates
Serial Issued date Expire date Subject Name
1 21:31:40 EST Jan 1 2020 21:31:40 EST Dec 31 2022 cn=IOS-CA


Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment url http://<local interface ip>:80
   # Replace <local interface ip> with the IP address of an interface on the r
Router(ca-trustpoint)# subject-name CN=TEST
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair TEST
Router(ca-trustpoint)# exit


Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki auth TEST
Certificate has the following attributes:
Fingerprint MD5: C281D9A0 337659CB D1B03AA6 11BD6E40
Fingerprint SHA1: 1779C425 3DCEE86D 2B11C880 D92361D6 8E2B71FF


% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.


Router(config)# crypto pki enroll TEST
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.


Password: <password>
Re-enter password: <password>


% The subject name in the certi
% The subject name in the certificate will include: Router.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: FTX1234ABCD
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose TEST' command will show the fingerp
```

Workaround 3

Use OpenSSL to generate a PKCS12 certificate bundle and import the bundle to Cisco IOS.

Note: This process generates a self-signed certificate and a corresponding key-pair package into a PKCS12 formatted file. This file is protected only by a password. Compromise of the password or of the key-pair itself will enable an unauthorized party to replicate this certificate. Appropriate steps should be taken to keep the key-pair and password confidential.

1. Generate a PKCS12 certificate bundle.
   Linux, UNIX, or macOS Example

```
User@linux-box$ openssl req -newkey rsa:2048 -nodes -keyout tmp.key -x509 -da
"/CN=SelfSignedCert" &> /dev/null && openssl pkcs12 -export -in tmp.cer -inke
-passout pass:<use a secure password> && openssl pkcs12 -export -out certific
-password pass:<use a secure password> -inkey
tmp.key -in tmp.cer && rm tmp.bin tmp.key tmp.cer && openssl base64 -in cert:


MIII8QIBAzCCCLcGCSqGSIb3DQEHAaCCCKgEggikMIIIoDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIGnxm
t5r28FECAggAgIIDEKyw10smucdQGt1c0DdfYXwUo8BwaBnzQvN0ClawXNQln2bT
vrhus6LfRvVxBNPeQz2ADgLikGxatwV5EDgooM+IEucKDURGLEotaRrVU5Wk3EGM
mjC6Ko9OaM30vhAGEEXrk26cq+OWsEuF3qudggRYv2gIBcrJ2iUQNFsBIrvlGHRo
FphOTqhVaAPxZS7hOB30cK1tMKHOIa8EwygyBvQPfjjBT79QFgeexIJFmUtqYX/P
<OUTPUT OMITTED FOR BREVITY>
tT6r4SuibYKu6HV45ffjSzOimcJI+D9LKhLWR6pK/k5ge8v7aK9/rsVbjavbdy7b
CSqGSIb3DQEJFTEWBBS96DY/gRfN1dSx46P1EqjPvSYiETAxMCEwCQYFKw4DAhoF
AAQU+EX0kNvuNz6XmFxXER8wlqKTGvgECA+D+Z81uwafAgIIAA==
```

2. Import the certificate to a Cisco IOS or Cisco IOS XE router.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki trustpoint TEST
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit


R1(config)#crypto pki import TEST pkcs12 terminal password <use a secure pas:
Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
MIII8QIBAzCCCLcGCSqGSIb3DQEHAaCCCKgEggikMIIIoDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQItyCo
Vh05+0QCAggAgIIDENUWY+UeuY5sIRZuoBi2nEhdIPd1th/auBYtX79aXGiz/iEW
<OUTPUT OMITTED FOR BREVITY>
IY1l273y9bC3qPVJ0UGoQW8SGfarqE
CsUVj+ll5hzGjK78L0ycXWpH4gDOGY
CSqGSIb3DQEJFTEWBBSgiBJIYpJLzo
AAQUdeUrLIC2uo/mbyE86he5+qEjmPYECKu/6GWaeKb/AgIIAA==
quit
CRYPTO_PKI: Imported PKCS12 file successfully.
R1(config)#
```

3. Verify that the new certificate is installed.

```
R1#show crypto pki certificates TEST

Load for five secs: 5%/1%; one minute: 2%; five minutes: 3%

Time source is SNTP, 15:04:37.593 UTC Mon Dec 16 2019

CA Certificate

  Status: Available

  Certificate Serial Number (hex): 00A16966E46A435A99

  Certificate Usage: General Purpose

  Issuer:

    cn=SelfSignedCert

  Subject:

    cn=SelfSignedCert

  Validity Date:

    start date: 14:54:46 UTC Dec 16 2019

end   date: 14:54:46 UTC Nov 28 2030
```

Workaround 4

Acquire a certificate from the customer's PKI using SCEP. This is a typical use case for utility customers. The steps to set up the IoT device to acquire a certificate from the customers PKI are:

1. Create a new trustpoint Locally Significant Device Identifier (LDevID).

```
crypto pki trustpoint LDevID
 enrollment retry count 10
 enrollment retry period 2
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password
 fingerprint 3F520C4C0F3236C9CA3D5C209C9948EC
 subject-name serialNumber=PID:IR829M-LTE-EA-AK9 SN:FTX2140Z04X,CN=FTX2140Z0
 revocation-check none
 rsakeypair LDevID 2048
```

2. Create an enrollment profile for the new trustpoint LDevID.

```
crypto pki profile enrollment LDevID
 enrollment url  http://192.168
```

3. Authenticate the trustpoint.

```
conf t
crypto pki authenticate LDevID
```

4. Enroll the trustpoint.

```
conf t
crypto pki enroll LDevID
```

5. Use the new LDevID certificate instead of SUDI for configurations and applications.

For More Information

If you require further assistance, or if you have any further questions regarding this field notice, please contact the Cisco Systems Technical Assistance Center (TAC) by one of the following methods:

- Open a service request on Cisco.com
- By email or telephone

Receive Email Notification For New Field Notices

My Notifications–Set up a profile to receive email updates about reliability, safety, network security, and end-of-sale issues for the Cisco products you specify.

Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap