Field Notice: FN - 70489 - PKI Self-Signed Certificate Expiration in Cisco IOS and

Updated: December 20, 2019 **Document ID:** FN70489

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	17-Dec-19	Initial Release
1.1	18-Dec-19	Minor text and formmatting correction
1.2	20-Dec-19	Updated information on WAAS, SSH example, ISAKMP/IKEv2 example, and solution guidance

Products Affected

Affected OS Type	Affected Software Product	Affected Release	Affected Release Number	Comments
IOS	IOS	15.6	15.6(1)S, 15.6(1)S1, 15.6(1)S2, 15.6(1)S3, 15.6(1)S4, 15.6(1)SN, 15.6(1)SN1, 15.6(1)T, 15.6(1)T0a, 15.6(1)T1, 15.6(1)T2, 15.6(1)T3, 15.6(2)S, 15.6(2)S1, 15.6(2)S2, 15.6(2)S3, 15.6(2)S4, 15.6(2)SP, 15.6(2)SP1, 15.6(2)SP2, 15.6(2)SP3, 15.6(2)SP4, 15.6(2)SP6, 15.6(2)T, 15.6(2)T0a, 15.6(2)T1, 15.6(2)T2, 15.6(2)T3, 15.6(3)M, 15.6(3)M0a, 15.6(3)M1, 15.6(3)M1a, 15.6(3)M1b, 15.6(3)M2, 15.6(3)M2a, 15.6(3)M3, 15.6(3)M3a, 15.6(3)M4, 15.6(3)M5, 15.6(3)M6, 15.6(3)M6a	All releases prior to 15.6(03)M07
IOS	IOS	15.7	15.7(3)M, 15.7(3)M1, 15.7(3)M2, 15.7(3)M3, 15.7(3)M4, 15.7(3)M4a, 15.7(3)M4b	All releases prior to 15.7(03)M05
IOS	IOS	15.8	15.8(3)M, 15.8(3)M0a, 15.8(3)M0b, 15.8(3)M1, 15.8(3)M1a, 15.8(3)M2,	All releases prior to 15.8(03)M03

			15.8(3)M2a	
IOS	IOS	15.9	15.9(3)M0a	All releases prior to 15.9(03)M
NON-IOS	IOSXE	16	16.1.0, 16.1.1, 16.1.2, 16.1.3, 16.2.1, 16.2.2, 16.3.1, 16.3.1a, 16.3.2, 16.3.3, 16.3.4, 16.3.5, 16.3.5b, 16.3.6, 16.3.7, 16.3.8, 16.3.9, 16.4.1, 16.4.2, 16.4.3, 16.5.1, 16.5.1a, 16.5.1b, 16.5.2, 16.5.3, 16.6.1, 16.6.1a, 16.6.2, 16.6.3, 16.6.4, 16.6.4a, 16.6.5, 16.6.5a, 16.6.6, 16.6.7, 16.7.1, 16.7.1a, 16.7.1b, 16.7.2, 16.7.3, 16.7.4, 16.8.1, 16.8.1a, 16.8.1b, 16.8.1c, 16.8.1d, 16.8.1e, 16.8.2, 16.8.3	All Cisco IOS XE releases prior to 16.9.1
IOS	IOS	15.5	15.5(1)S, 15.5(1)S1, 15.5(1)S2, 15.5(1)S3, 15.5(1)S4, 15.5(1)SY, 15.5(1)SY1, 15.5(1)SY2, 15.5(1)SY3, 15.5(1)SY4, 15.5(1)T, 15.5(1)T1, 15.5(1)T2, 15.5(1)T3, 15.5(1)T4, 15.5(2)S, 15.5(2)S1, 15.5(2)S2, 15.5(2)S3, 15.5(2)S4, 15.5(2)T, 15.5(2)T1, 15.5(2)T2, 15.5(2)T3, 15.5(2)T4, 15.5(2)XB, 15.5(3)M, 15.5(3)M0a, 15.5(3)M1, 15.5(3)M10, 15.5(3)M2, 15.5(3)M2a, 15.5(3)M3, 15.5(3)M4, 15.5(3)M4a, 15.5(3)M4b, 15.5(3)M4c, 15.5(3)M5, 15.5(3)M5a, 15.5(3)M6, 15.5(3)M6a, 15.5(3)M7, 15.5(3)M8, 15.5(3)M9, 15.5(3)S, 15.5(3)S0a, 15.5(3)S1, 15.5(3)S10, 15.5(3)S1a, 15.5(3)S2, 15.5(3)S3, 15.5(3)S4, 15.5(3)S5, 15.5(3)S6b, 15.5(3)S7, 15.5(3)S8, 15.5(3)S9, 15.5(3)S9a, 15.5(3)SN	All versions of Cisco IOS 15.5 are affected
IOS	IOS	15.4	15.4(1)CG, 15.4(1)CG1, 15.4(1)S, 15.4(1)S0a, 15.4(1)S0b, 15.4(1)S0c, 15.4(1)S1, 15.4(1)S2, 15.4(1)S3, 15.4(1)S4, 15.4(1)SY, 15.4(1)SY1,	All versions of Cisco IOS 15.4 are affected

			15.4(1)SY2, 15.4(1)SY4, 15.4(1)T, 15.4(1)T1, 15.4(1)T2, 15.4(1)T3, 15.4(1)T4, 15.4(2)CG, 15.4(2)S, 15.4(2)S1, 15.4(2)S2, 15.4(2)S3, 15.4(2)S4, 15.4(2)SN, 15.4(2)SN1, 15.4(2)T, 15.4(2)T1, 15.4(2)T2, 15.4(2)T3, 15.4(2)T4, 15.4(3)M, 15.4(3)M1, 15.4(3)M10, 15.4(3)M2, 15.4(3)M3, 15.4(3)M4, 15.4(3)M5, 15.4(3)M6, 15.4(3)M6a, 15.4(3)M7, 15.4(3)M7a, 15.4(3)M8, 15.4(3)M9, 15.4(3)S, 15.4(3)S1, 15.4(3)S2, 15.4(3)S3, 15.4(3)S4, 15.4(3)S5, 15.4(3)S6, 15.4(3)S6a, 15.4(3)S7, 15.4(3)S8, 15.4(3)S9, 15.4(3)SN1	
IOS	IOS	15.3	15.3(0)SY, 15.3(1)S, 15.3(1)S1, 15.3(1)S1e, 15.3(1)S2, 15.3(1)SY, 15.3(1)SY1, 15.3(1)SY2, 15.3(1)T, 15.3(1)T1, 15.3(1)T2, 15.3(1)T3, 15.3(1)T4, 15.3(2)S, 15.3(2)S1, 15.3(2)S1b, 15.3(2)S1c, 15.3(2)S2, 15.3(2)T, 15.3(2)T1, 15.3(2)T2, 15.3(2)T3, 15.3(2)T4, 15.3(3)JA1, 15.3(3)JA10, 15.3(3)JA11, 15.3(3)JA12, 15.3(3)JA1m, 15.3(3)JA4, 15.3(3)JA5, 15.3(3)JA7, 15.3(3)JA8, 15.3(3)JA9, 15.3(3)JAA, 15.3(3)JAB, 15.3(3)JAX, 15.3(3)JAX1, 15.3(3)JAX2, 15.3(3)JB, 15.3(3)JBB, 15.3(3)JBB1, 15.3(3)JBB2, 15.3(3)JBB4, 15.3(3)JBB5, 15.3(3)JBB6, 15.3(3)JC, 15.3(3)JC1, 15.3(3)JC14, 15.3(3)JC15, 15.3(3)JC2, 15.3(3)JC3,	All versions of Cisco IOS 15.3 are affected

			15.3(3)JC4, 15.3(3)JC5, 15.3(3)JC50, 15.3(3)JC6, 15.3(3)JC7, 15.3(3)JC8, 15.3(3)JC9, 15.3(3)JD, 15.3(3)JD11, 15.3(3)JD12, 15.3(3)JD13, 15.3(3)JD14, 15.3(3)JD16, 15.3(3)JD17, 15.3(3)JD2, 15.3(3)JD3, 15.3(3)JD4, 15.3(3)JD5, 15.3(3)JD6, 15.3(3)JD7, 15.3(3)JD8, 15.3(3)JD9, 15.3(3)JE, 15.3(3)JF, 15.3(3)JF1, 15.3(3)JF10, 15.3(3)JF11, 15.3(3)JF4, 15.3(3)JF5, 15.3(3)JF7, 15.3(3)JF8, 15.3(3)JF9, 15.3(3)JG1, 15.3(3)JH, 15.3(3)JH1, 15.3(3)JI1, 15.3(3)JI3, 15.3(3)JI4, 15.3(3)JI5, 15.3(3)JJ, 15.3(3)JJ1, 15.3(3)JK, 15.3(3)M, 15.3(3)M1, 15.3(3)M10, 15.3(3)M2, 15.3(3)M3, 15.3(3)M4, 15.3(3)M5, 15.3(3)M6, 15.3(3)M7, 15.3(3)M8, 15.3(3)M8a, 15.3(3)M9, 15.3(3)S, 15.3(3)S1, 15.3(3)S10, 15.3(3)S1a, 15.3(3)S2, 15.3(3)S2a, 15.3(3)S3, 15.3(3)S4, 15.3(3)S5, 15.3(3)S6, 15.3(3)S6a, 15.3(3)S7, 15.3(3)S8, 15.3(3)S8a, 15.3(3)S9, 15.3(3)XB12	
IOS	IOS	15.2	15.2(1)E, 15.2(1)E1, 15.2(1)E2, 15.2(1)E3, 15.2(1)EY, 15.2(1)GC, 15.2(1)GC1, 15.2(1)GC2, 15.2(1)S, 15.2(1)S1, 15.2(1)S2, 15.2(1)SY, 15.2(1)SY0a, 15.2(1)SY1, 15.2(1)SY1a, 15.2(1)SY2, 15.2(1)SY3, 15.2(1)SY4, 15.2(1)SY5, 15.2(1)SY6, 15.2(1)SY7,	All versions of Cisco IOS 15.2 are affected

			15.2(1)SY8, 15.2(1)T, 15.2(1)T1, 15.2(1)T2, 15.2(1)T3, 15.2(1)T3a, 15.2(1)T4, 15.2(2)E, 15.2(2)E1, 15.2(2)E10, 15.2(2)E2, 15.2(2)E3, 15.2(2)E4, 15.2(2)E5, 15.2(2)E5a, 15.2(2)E6, 15.2(2)E7, 15.2(2)E8, 15.2(2)E9, 15.2(2)E9a, 15.2(2)EA, 15.2(2)EA1, 15.2(2)EA2, 15.2(2)EA3, 15.2(2)EB, 15.2(2)EB1, 15.2(2)EB2, 15.2(2)GC, 15.2(2)JA1, 15.2(2)JAX, 15.2(2)JB, 15.2(2)JB2, 15.2(2)JB3, 15.2(2)JB4, 15.2(2)JB5, 15.2(2)JB6, 15.2(2)S, 15.2(2)S0a, 15.2(2)S0c, 15.2(2)S0d, 15.2(2)S1, 15.2(2)S2, 15.2(2)SA, 15.2(2)SA1, 15.2(2)SA2, 15.2(2)SNG, 15.2(2)SNH, 15.2(2)SNH1, 15.2(2)SNI, 15.2(2)SY, 15.2(2)SY1, 15.2(2)SY2, 15.2(2)SY3, 15.2(2)T, 15.2(2)T1, 15.2(2)T2, 15.2(2)T3, 15.2(2)T4, 15.2(2b)E, 15.2(3)E, 15.2(3)E1, 15.2(3)E2, 15.2(3)E3, 15.2(3)EA, 15.2(3)GC, 15.2(3)GC1, 15.2(3)GCA, 15.2(3)GCA1, 15.2(3)T, 15.2(3)T1, 15.2(3)T2, 15.2(3)T4, 15.2(3)XA, 15.2(4)E, 15.2(4)E1, 15.2(4)E2, 15.2(4)E3, 15.2(4)E4, 15.2(4)E5, 15.2(4)E6, 15.2(4)E7, 15.2(4)E8, 15.2(4)E9, 15.2(4)EA, 15.2(4)EA1, 15.2(4)EA2, 15.2(4)EA3, 15.2(4)EA4, 15.2(4)EA5, 15.2(4)EA7, 15.2(4)EA8, 15.2(4)EA9, 15.2(4)EB, 15.2(4)EC, 15.2(4)EC1, 15.2(4)EC2, 15.2(4)GC, 15.2(4)GC1, 15.2(4)GC2, 15.2(4)GC3, 15.2(4)JA, 15.2(4)JA1, 15.2(4)JB, 15.2(4)JB1, 15.2(4)JB3a,	

			15.2(4)JB3b, 15.2(4)JB4, 15.2(4)JB5, 15.2(4)JB6, 15.2(4)M, 15.2(4)M1, 15.2(4)M10, 15.2(4)M11, 15.2(4)M2, 15.2(4)M3, 15.2(4)M4, 15.2(4)M5, 15.2(4)M6, 15.2(4)M6a, 15.2(4)M6b, 15.2(4)M7, 15.2(4)M8, 15.2(4)M9, 15.2(4)S, 15.2(4)S0c, 15.2(4)S1, 15.2(4)S1c, 15.2(4)S2, 15.2(4)S3, 15.2(4)S3a, 15.2(4)S4, 15.2(4)S4a, 15.2(4)S5, 15.2(4)S6, 15.2(4)S7, 15.2(4)S8, 15.2(4)XB10, 15.2(4)XB11, 15.2(4)XB9, 15.2(4a)EA5, 15.2(5)E, 15.2(5)E1, 15.2(5)E2, 15.2(5)E2a, 15.2(5)E2c, 15.2(5)EA, 15.2(5a)E1, 15.2(6)E, 15.2(6)E1, 15.2(6)E1s, 15.2(6)E3, 15.2(7)E, 15.2(7)E0s	
IOS	IOS	15.1	15.1(1)MR, 15.1(1)MR3, 15.1(1)S, 15.1(1)S1, 15.1(1)S2, 15.1(1)SG, 15.1(1)SG1, 15.1(1)SG2, 15.1(1)SY, 15.1(1)SY1, 15.1(1)SY2, 15.1(1)SY3, 15.1(1)SY4, 15.1(1)SY5, 15.1(1)SY6, 15.1(1)T, 15.1(1)T1, 15.1(1)T2, 15.1(1)T3, 15.1(1)T4, 15.1(1)T5, 15.1(1)XB, 15.1(1)XB1, 15.1(1)XB2, 15.1(1)XB3, 15.1(2)EY, 15.1(2)EY1, 15.1(2)EY1a, 15.1(2)EY2, 15.1(2)EY2a, 15.1(2)EY3, 15.1(2)EY4, 15.1(2)GC, 15.1(2)GC1, 15.1(2)GC2, 15.1(2)S, 15.1(2)S1, 15.1(2)S2, 15.1(2)SG, 15.1(2)SG1, 15.1(2)SG2, 15.1(2)SG3, 15.1(2)SG4, 15.1(2)SG5, 15.1(2)SG6, 15.1(2)SG7, 15.1(2)SG8, 15.1(2)SNG,	All versions of Cisco IOS 15.1 are affected

			15.1(2)SNH, 15.1(2)SNI, 15.1(2)SNI1, 15.1(2)SY, 15.1(2)SY1, 15.1(2)SY10, 15.1(2)SY11, 15.1(2)SY12, 15.1(2)SY13, 15.1(2)SY14, 15.1(2)SY15, 15.1(2)SY2, 15.1(2)SY3, 15.1(2)SY4, 15.1(2)SY4a, 15.1(2)SY5, 15.1(2)SY6, 15.1(2)SY7, 15.1(2)SY8, 15.1(2)SY9, 15.1(2)T, 15.1(2)T0a, 15.1(2)T1, 15.1(2)T2, 15.1(2)T2a, 15.1(2)T3, 15.1(2)T4, 15.1(2)T5, 15.1(3)MR, 15.1(3)MRA, 15.1(3)S, 15.1(3)S0a, 15.1(3)S1, 15.1(3)S2, 15.1(3)S3, 15.1(3)S4, 15.1(3)S5, 15.1(3)S5a, 15.1(3)S6, 15.1(3)S7, 15.1(3)T, 15.1(3)T1, 15.1(3)T2, 15.1(3)T3, 15.1(3)T4, 15.1(4)GC, 15.1(4)GC1, 15.1(4)GC2, 15.1(4)M, 15.1(4)M0a, 15.1(4)M0b, 15.1(4)M1, 15.1(4)M10, 15.1(4)M11, 15.1(4)M12, 15.1(4)M12a, 15.1(4)M2, 15.1(4)M3, 15.1(4)M3a, 15.1(4)M4, 15.1(4)M5, 15.1(4)M6, 15.1(4)M7, 15.1(4)M8, 15.1(4)M9, 15.1(4)XB4, 15.1(4)XB5, 15.1(4)XB5a, 15.1(4)XB6, 15.1(4)XB7, 15.1(4)XB8, 15.1(4)XB8a	
IOS	IOS	15.0	15.0(1)EY, 15.0(1)M, 15.0(1)M1, 15.0(1)M10, 15.0(1)M2, 15.0(1)M3, 15.0(1)M4, 15.0(1)M5, 15.0(1)M6, 15.0(1)M6a, 15.0(1)M7, 15.0(1)M8, 15.0(1)M9, 15.0(1)MR, 15.0(1)S, 15.0(1)S1, 15.0(1)S2, 15.0(1)S3a, 15.0(1)S4, 15.0(1)S4a, 15.0(1)S5, 15.0(1)S6,	All versions of Cisco IOS 15.0 are affected

			15.0(1)SE, 15.0(1)SE1, 15.0(1)SE2, 15.0(1)SE3, 15.0(1)SY, 15.0(1)SY1, 15.0(1)SY10, 15.0(1)SY2, 15.0(1)SY3, 15.0(1)SY4, 15.0(1)SY5, 15.0(1)SY6, 15.0(1)SY7, 15.0(1)SY7a, 15.0(1)SY8, 15.0(1)SY9, 15.0(1)XA, 15.0(1)XA1, 15.0(1)XA2, 15.0(1)XA3, 15.0(1)XA4, 15.0(1)XA5, 15.0(2)EA, 15.0(2)EA1, 15.0(2)EB, 15.0(2)EC, 15.0(2)ED, 15.0(2)ED1, 15.0(2)EH, 15.0(2)EJ, 15.0(2)EJ1, 15.0(2)EK, 15.0(2)EK1, 15.0(2)EY, 15.0(2)EY1, 15.0(2)EY2, 15.0(2)EY3, 15.0(2)EZ, 15.0(2)MR, 15.0(2)SE, 15.0(2)SE1, 15.0(2)SE10, 15.0(2)SE10a, 15.0(2)SE11, 15.0(2)SE12, 15.0(2)SE13, 15.0(2)SE2, 15.0(2)SE3, 15.0(2)SE4, 15.0(2)SE5, 15.0(2)SE6, 15.0(2)SE7, 15.0(2)SE8, 15.0(2)SE9, 15.0(2)SG, 15.0(2)SG1, 15.0(2)SG10, 15.0(2)SG11, 15.0(2)SG2, 15.0(2)SG3, 15.0(2)SG4, 15.0(2)SG5, 15.0(2)SG6, 15.0(2)SG7, 15.0(2)SG8, 15.0(2)SG9, 15.0(2a)SE6, 15.0(2a)SE9	
IOS	IOS	12.4	12.4(1), 12.4(10), 12.4(10a), 12.4(10b), 12.4(10b)JA, 12.4(10b)JA1, 12.4(10b)JA3, 12.4(10b)JDA, 12.4(10b)JDA3, 12.4(10b)JX, 12.4(10b)JY, 12.4(10c), 12.4(11)MD10, 12.4(11)MD3, 12.4(11)MD4,	All versions of Cisco IOS version 12.x are affected

			12.4(11)MD5, 12.4(11)MD6, 12.4(11)MD7, 12.4(11)MD8, 12.4(11)MD9, 12.4(11)MR, 12.4(11)SW, 12.4(11)SW1, 12.4(11)SW2, 12.4(11)SW3, 12.4(11)T, 12.4(11)T1, 12.4(11)T2, 12.4(11)T3, 12.4(11)T4, 12.4(11)XJ, 12.4(11)XJ1, 12.4(11)XJ2, 12.4(11)XJ3, 12.4(11)XJ4, 12.4(11)XJ5, 12.4(11)XJ6, 12.4(11)XV, 12.4(11)XV1, 12.4(11)XW, 12.4(11)XW1, 12.4(11)XW10, 12.4(11)XW2, 12.4(11)XW3, 12.4(11)XW4, 12.4(11)XW5, 12.4(11)XW6, 12.4(11)XW7, 12.4(11)XW8, 12.4(11)XW9, 12.4(12), 12.4(12)MR, 12.4(12)MR1, 12.4(12)MR2, 12.4(12a), 12.4(12b), 12.4(12c), 12.4(13), 12.4(13a), 12.4(13b), 12.4(13c), 12.4(13d), 12.4(13d)JA, 12.4(13e), 12.4(13f), 12.4(14)XK, 12.4(15)MD, 12.4(15)MD1, 12.4(15)MD1a, 12.4(15)MD2, 12.4(15)MD3, 12.4(15)MD4, 12.4(15)MD5, 12.4(15)SW, 12.4(15)SW1, 12.4(15)SW2, 12.4(15)SW3, 12.4(15)SW4, 12.4(15)SW5, 12.4(15)SW6, 12.4(15)SW7, 12.4(15)SW8, 12.4(15)SW8a, 12.4(15)SW9, 12.4(15)T, 12.4(15)T1, 12.4(15)T10, 12.4(15)T11,	

			12.4(15)T12, 12.4(15)T13, 12.4(15)T13b, 12.4(15)T14, 12.4(15)T15, 12.4(15)T16, 12.4(15)T17, 12.4(15)T2, 12.4(15)T3, 12.4(15)T4, 12.4(15)T5, 12.4(15)T6, 12.4(15)T6a, 12.4(15)T7, 12.4(15)T8, 12.4(15)T9, 12.4(15)XL, 12.4(15)XL1, 12.4(15)XL2, 12.4(15)XL3, 12.4(15)XL4, 12.4(15)XL5, 12.4(15)XM, 12.4(15)XM1, 12.4(15)XM2, 12.4(15)XM3, 12.4(15)XN, 12.4(15)XQ, 12.4(15)XQ1, 12.4(15)XQ2, 12.4(15)XQ2a, 12.4(15)XQ2b, 12.4(15)XQ2c, 12.4(15)XQ2d, 12.4(15)XQ3, 12.4(15)XQ4, 12.4(15)XQ5, 12.4(15)XQ6, 12.4(15)XQ7, 12.4(15)XQ8, 12.4(15)XR, 12.4(15)XR1, 12.4(15)XR10, 12.4(15)XR2, 12.4(15)XR3, 12.4(15)XR4, 12.4(15)XR5, 12.4(15)XR6, 12.4(15)XR7, 12.4(15)XR8, 12.4(15)XR9, 12.4(15)XY, 12.4(15)XY1, 12.4(15)XY2, 12.4(15)XY3, 12.4(15)XY4, 12.4(15)XY5, 12.4(15)XZ, 12.4(15)XZ1, 12.4(15)XZ2, 12.4(16), 12.4(16)MR, 12.4(16)MR1, 12.4(16)MR2, 12.4(16a), 12.4(16b), 12.4(17), 12.4(17a), 12.4(17b), 12.4(18),	

			12.4(18a), 12.4(18a)JA1, 12.4(18b), 12.4(18c), 12.4(18d), 12.4(18e), 12.4(19), 12.4(19)MR, 12.4(19)MR1, 12.4(19)MR2, 12.4(19)MR3, 12.4(19b), 12.4(1a), 12.4(1b), 12.4(1c), 12.4(2)MR, 12.4(2)MR1, 12.4(2)T, 12.4(2)T1, 12.4(2)T2, 12.4(2)T3, 12.4(2)T4, 12.4(2)T5, 12.4(2)T6, 12.4(2)XA, 12.4(2)XA1, 12.4(2)XA2, 12.4(2)XB, 12.4(2)XB1, 12.4(2)XB10, 12.4(2)XB11, 12.4(2)XB2, 12.4(2)XB3, 12.4(2)XB4, 12.4(2)XB5, 12.4(2)XB6, 12.4(2)XB7, 12.4(2)XB8, 12.4(2)XB9, 12.4(20)MR, 12.4(20)MR1, 12.4(20)MR2, 12.4(20)MRA, 12.4(20)MRA1, 12.4(20)MRB, 12.4(20)MRB1, 12.4(20)T, 12.4(20)T1, 12.4(20)T2, 12.4(20)T3, 12.4(20)T4, 12.4(20)T5, 12.4(20)T5a, 12.4(20)T6, 12.4(20)T7, 12.4(20)T8, 12.4(20)T9, 12.4(20)YA, 12.4(20)YA1, 12.4(20)YA2, 12.4(20)YA3, 12.4(21), 12.4(21a), 12.4(21a)JA, 12.4(21a)JA1, 12.4(21a)JA2, 12.4(21a)JX, 12.4(21a)JY, 12.4(21a)JZ, 12.4(21a)M1, 12.4(22)GC1, 12.4(22)GC1a, 12.4(22)MD, 12.4(22)MD1, 12.4(22)MD2, 12.4(22)MDA, 12.4(22)MDA1, 12.4(22)MDA2, 12.4(22)MDA3, 12.4(22)MDA4,	

			12.4(22)MDA5, 12.4(22)MDA6, 12.4(22)T, 12.4(22)T1, 12.4(22)T2, 12.4(22)T3, 12.4(22)T4, 12.4(22)T5, 12.4(22)XR, 12.4(22)XR11, 12.4(22)XR12, 12.4(22)YB, 12.4(22)YB1, 12.4(22)YB3, 12.4(22)YB4, 12.4(22)YB5, 12.4(22)YB6, 12.4(22)YB7, 12.4(22)YB8, 12.4(22)YD, 12.4(22)YD1, 12.4(22)YD2, 12.4(22)YD3, 12.4(22)YD4, 12.4(22)YE, 12.4(22)YE1, 12.4(22)YE2, 12.4(22)YE3, 12.4(22)YE4, 12.4(22)YE5, 12.4(22)YE6, 12.4(23), 12.4(23a), 12.4(23b), 12.4(23b)M1, 12.4(23c), 12.4(23c)JA, 12.4(23c)JA10, 12.4(23c)JA2, 12.4(23c)JA3, 12.4(23c)JA4, 12.4(23c)JA5, 12.4(23c)JA7, 12.4(23c)JA8, 12.4(23c)JA9, 12.4(23c)JY, 12.4(23d), 12.4(23e), 12.4(24)GC1, 12.4(24)GC3, 12.4(24)GC3a, 12.4(24)GC4, 12.4(24)GC5, 12.4(24)MD, 12.4(24)MD1, 12.4(24)MD2, 12.4(24)MD3, 12.4(24)MD4, 12.4(24)MD5, 12.4(24)MD6, 12.4(24)MD7, 12.4(24)MDA, 12.4(24)MDA1, 12.4(24)MDA10, 12.4(24)MDA11, 12.4(24)MDA12, 12.4(24)MDA13, 12.4(24)MDA2, 12.4(24)MDA3,	

			12.4(24)MDA4, 12.4(24)MDA5, 12.4(24)MDA6, 12.4(24)MDA7, 12.4(24)MDA8, 12.4(24)MDA9, 12.4(24)MDB, 12.4(24)MDB1, 12.4(24)MDB10, 12.4(24)MDB11, 12.4(24)MDB12, 12.4(24)MDB13, 12.4(24)MDB14, 12.4(24)MDB15, 12.4(24)MDB16, 12.4(24)MDB17, 12.4(24)MDB18, 12.4(24)MDB19, 12.4(24)MDB3, 12.4(24)MDB4, 12.4(24)MDB5, 12.4(24)MDB5a, 12.4(24)MDB6, 12.4(24)MDB7, 12.4(24)MDB8, 12.4(24)MDB9, 12.4(24)T, 12.4(24)T1, 12.4(24)T10, 12.4(24)T11, 12.4(24)T12, 12.4(24)T2, 12.4(24)T3, 12.4(24)T31f, 12.4(24)T32f, 12.4(24)T33f, 12.4(24)T34d, 12.4(24)T34f, 12.4(24)T35c, 12.4(24)T35f, 12.4(24)T3a, 12.4(24)T3b, 12.4(24)T3c, 12.4(24)T3e, 12.4(24)T3f, 12.4(24)T4, 12.4(24)T4a, 12.4(24)T4b, 12.4(24)T4c, 12.4(24)T4d, 12.4(24)T4e, 12.4(24)T4f, 12.4(24)T4g, 12.4(24)T4h, 12.4(24)T4i, 12.4(24)T4j, 12.4(24)T4k, 12.4(24)T4l, 12.4(24)T4m, 12.4(24)T4n, 12.4(24)T4o, 12.4(24)T5, 12.4(24)T6, 12.4(24)T7, 12.4(24)T8, 12.4(24)T9, 12.4(24)YE,	

			12.4(24)YE1, 12.4(24)YE2, 12.4(24)YE3, 12.4(24)YE3a, 12.4(24)YE3b, 12.4(24)YE3c, 12.4(24)YE3d, 12.4(24)YE3e, 12.4(24)YE4, 12.4(24)YE5, 12.4(24)YE6, 12.4(24)YE7, 12.4(24)YG, 12.4(24)YG1, 12.4(24)YG2, 12.4(24)YG3, 12.4(24)YG4, 12.4(24)YS, 12.4(24)YS1, 12.4(24)YS10, 12.4(24)YS2, 12.4(24)YS3, 12.4(24)YS4, 12.4(24)YS5, 12.4(24)YS6, 12.4(24)YS7, 12.4(24)YS8, 12.4(24)YS8a, 12.4(24)YS9, 12.4(25), 12.4(25a), 12.4(25b), 12.4(25c), 12.4(25d), 12.4(25d)JA, 12.4(25d)JA1, 12.4(25d)JA2, 12.4(25d)JAX, 12.4(25d)JAX1, 12.4(25d)JB, 12.4(25e), 12.4(25e)JA, 12.4(25e)JAL, 12.4(25e)JAL2, 12.4(25e)JAM, 12.4(25e)JAM2, 12.4(25e)JAM3, 12.4(25e)JAM4, 12.4(25e)JAM5, 12.4(25e)JAM6, 12.4(25e)JAN, 12.4(25e)JAN1, 12.4(25e)JAO, 12.4(25e)JAO1, 12.4(25e)JAO3, 12.4(25e)JAO4, 12.4(25e)JAO5, 12.4(25e)JAO6, 12.4(25e)JAP, 12.4(25e)JAP1, 12.4(25e)JAP10, 12.4(25e)JAP11, 12.4(25e)JAP12, 12.4(25e)JAP4, 12.4(25e)JAP5, 12.4(25e)JAP7,	

			12.4(25e)JAP8, 12.4(25e)JAP9, 12.4(25e)JAX, 12.4(25e)JAX1, 12.4(25e)JAX2, 12.4(25e)JAZ, 12.4(25e)JX, 12.4(25f), 12.4(25g), 12.4(3), 12.4(3)JK, 12.4(3)JK1, 12.4(3)JK2, 12.4(3)JK3, 12.4(3)JK4, 12.4(3)JL, 12.4(3)JL1, 12.4(3)JL2, 12.4(3a), 12.4(3b), 12.4(3c), 12.4(3d), 12.4(3e), 12.4(3f), 12.4(3g), 12.4(3g)JA, 12.4(3g)JA1, 12.4(3g)JMA, 12.4(3g)JX, 12.4(3g)JX1, 12.4(3g)JX2, 12.4(3h), 12.4(3i), 12.4(3j), 12.4(4)MR, 12.4(4)MR1, 12.4(4)T, 12.4(4)T1, 12.4(4)T2, 12.4(4)T3, 12.4(4)T4, 12.4(4)T5, 12.4(4)T6, 12.4(4)T7, 12.4(4)T8, 12.4(4)XC, 12.4(4)XC1, 12.4(4)XC2, 12.4(4)XC3, 12.4(4)XC4, 12.4(4)XC5, 12.4(4)XC6, 12.4(4)XC7, 12.4(4)XD, 12.4(4)XD1, 12.4(4)XD10, 12.4(4)XD11, 12.4(4)XD12, 12.4(4)XD2, 12.4(4)XD3, 12.4(4)XD4, 12.4(4)XD5, 12.4(4)XD6, 12.4(4)XD7, 12.4(4)XD8, 12.4(4)XD9, 12.4(5), 12.4(5a), 12.4(5a)M0, 12.4(5b), 12.4(5c), 12.4(6)MR, 12.4(6)MR1, 12.4(6)T, 12.4(6)T1, 12.4(6)T10, 12.4(6)T11, 12.4(6)T12, 12.4(6)T2, 12.4(6)T3, 12.4(6)T4, 12.4(6)T5, 12.4(6)T5a, 12.4(6)T5b, 12.4(6)T5c, 12.4(6)T5d, 12.4(6)T5e, 12.4(6)T5f, 12.4(6)T6, 12.4(6)T7, 12.4(6)T8, 12.4(6)T9, 12.4(6)XE, 12.4(6)XE1, 12.4(6)XE2, 12.4(6)XE3, 12.4(6)XP,	

			12.4(6)XT, 12.4(6)XT1, 12.4(6)XT2, 12.4(7), 12.4(7a), 12.4(7b), 12.4(7c), 12.4(7d), 12.4(7e), 12.4(7f), 12.4(7g), 12.4(7h), 12.4(8), 12.4(8a), 12.4(8b), 12.4(8c), 12.4(8d), 12.4(9)MR, 12.4(9)T, 12.4(9)T1, 12.4(9)T2, 12.4(9)T3, 12.4(9)T4, 12.4(9)T5, 12.4(9)T6, 12.4(9)T7, 12.4(9)XG3, 12.4(9)XG4, 12.4(9)XG5	

Defect Information

Defect ID	Headline
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time

Problem Description

Self-signed X.509 PKI certificates (SSC) that were generated on devices that run affected Cisco IOS® or Cisco IOS XE software releases expire on 2020-01-01 00:00:00 UTC. New self-signed certificates cannot be created on affected devices after 2020-01-01 00:00:00 UTC. Any service that relies on these self-signed certificates to establish or terminate a secure connection might not work after the certificate expires.

This issue affects only self-signed certificates that were generated by the Cisco IOS or Cisco IOS XE device and applied to a service on the device. Certificates that were generated by a Certificate Authority (CA), which includes those certificates generated by the Cisco IOS CA feature, are not impacted by this issue.

Note: To be impacted by this issue, a device must have a self-signed certificate defined *AND* the self-signed certificate must be applied to one or more features as outlined below. Presence of a self-signed certificate alone will not impact the operation of the device when the certificate expires and does not require immediate action.

Background

Certain features in Cisco IOS and Cisco IOS XE software rely on digitally signed X.509 certificates for cryptographic identity validation. These certificates can be generated by an external third-party CA or they can be generated on the Cisco IOS or Cisco IOS XE device itself as a self-signed certificate. Affected releases of Cisco IOS and Cisco IOS XE software will always set the expiration date of the self-signed certificate to 2020-01-01 00:00:00 UTC. After this date, the certificate expires and is invalid.

Note: A Cisco IOS or Cisco IOS XE device does not have to run an affected software version in order for its SSC to expire. All PKI certificates eventually expire. An SSC might have been generated and installed when the device previously ran an impacted software version. It is a recommended best-practice to monitor certificate expiration dates on all devices, even those that run software with the fix applied.

Services that might rely on a self-signed certificate include:

General Features:

- HTTP Server over TLS (HTTPS) - HTTPS will produce an error in the browser which indicates that the certificate is expired.
- SSH Server - Users who use X.509 certificates to authenticate the SSH session might fail to authenticate. (This use of X.509 certificates is rare. Username/password authentication and public/private key authentication are not affected.)
- RESTCONF - RESTCONF connections might fail.

Collaboration Features:

- Session Initiation Protocol (SIP) over TLS
- Cisco Unified Communications Manager Express (CME) with encrypted signaling enabled
- Cisco Unified Survivable Remote Site Telephony (SRST) with encrypted signaling enabled
- Cisco IOS dspfarm resources (Conference, Media Termination Point, or Transcoding) with encrypted signaling enabled
- Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) ports configured with encrypted signaling
- Media Gateway Control Protocol (MGCP) and H.323 call signaling over IP security (IPSec) without a pre-shared key
- Cisco Unified Communications Gateway Services API in Secure Mode (using HTTPS)

Wireless Features:

- LWAPP/CAPWAP connections between older Cisco IOS access points (manufactured in 2005 or earlier) and Wireless LAN Controllers; see Cisco Field Notice FN63942 for more details.

WAN Features:

- WAAS - New routers cannot be added to a WAAS Central Manager after the self-signed certificate expires. Existing routers are not affected.

Problem Symptom

An attempt to generate a self-signed certificate on an affected Cisco IOS or Cisco IOS XE software release after 2020-01-01 00:00:00 UTC results in this error:

```
../cert-c/source/certobj.c(535) : E_VALIDITY : validity period start later than end
```

Any services that rely on the self-signed certificate will be affected. For example:

- SIP over TLS calls will not complete.
- Devices registered to Cisco Unified CME with encrypted signaling enabled will no longer function.
- Cisco Unified SRST with encrypted signaling enabled will not allow devices to register.
- Cisco IOS dspfarm resources (Conference, Media Termination Point, or Transcoding) with encrypted signaling enabled will no longer register.
- STCAPP ports configured with encrypted signaling will no longer register.
- Calls through a gateway using MGCP or H.323 call signaling over IPSec without a pre-shared key will fail.
- API calls that use the Cisco Unified Communications Gateway Services API in Secure Mode (using HTTPS) will fail.
- RESTCONF might fail.
- HTTPS sessions to manage the device will display a browser warning which indicates that the certificate has expired.
- AnyConnect SSL VPN sessions will fail to establish or report an invalid certificate.
- IPSec connections will fail to establish.

Workaround/Solution

The solution is to deploy one of the workarounds described below or upgrade the Cisco IOS or Cisco IOS XE software to a release that includes the fix:

- Cisco IOS XE Software Release 16.9.1 and later
- Cisco IOS Software Release 15.6(3)M7 and later; 15.7(3)M5 and later; or 15.8(3)M3 and later

After you upgrade the software, you must *ALSO* regenerate the self-signed certificate and export it to any devices that might require the new certificate in their trust-store.

The three workarounds that are described below are just as effective as a software upgrade and are the preferred solution if an immediate software upgrade is not feasible.

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 considered to be 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 lines.
-----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 being used. Consult the documentation for 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
```

5.
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, keys will be non-exportable...
[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 router
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: <passsword>
Re-enter password: <password>

% The subject name in the certificate will include: CN=TEST
% 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 fingerprint.
```

Workaround 3

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

1. Generate a PKCS12 certificate bundle:

Linux, UNIX, or macOS example

```
User@linux-box$ openssl req -newkey rsa:2048 -nodes -keyout tmp.key -x509 -days 4000 -out tmp.cer -
subj
"/CN=SelfSignedCert" &> /dev/null && openssl pkcs12 -export -in tmp.cer -inkey tmp.key -out tmp.bin
-passout pass:Cisco123 && openssl pkcs12 -export -out certificate.pfx -password pass:Cisco123 -inkey
tmp.key -in tmp.cer && rm tmp.bin tmp.key tmp.cer && openssl base64 -in certificate.pfx

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 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 Cisco123
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>
IY1l273y9bC3qPVJ0UGoQW8SGfarqEjaqxdAet66E5V6u9Yvd4oMsIYGsa70m+FN
CsUVj+ll5hzGjK78L0ycXWpH4gDOGYBVf+D7mgWqaqZvxYUoEkOrTMmW5zElMCMG
CSqGSIb3DQEJFTEWBBSgiBJIYpJLzo/GYN0sesZh3wGmPTAxMCEwCQYFKw4DAhoF
AAQUdeUrLIC2uo/mbyE86he5+qEjmPYECKu76GWaeKb7AgIIAA==
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
```

How To Identify Affected Products

Note: To be impacted by this field notice, a device must have a self-signed certificate defined *AND* the self-signed certificate must be applied to one or more features as outlined below. Presence of a self-signed certificate alone will not impact the operation of the device when the certificate expires and does not require immediate action. To be impacted, a device must meet the criteria in *BOTH* Step 3 and Step 4 below.

In order to determine if you use a self-signed certificate, complete these steps:

1.
Enter the **show running-config | begin crypto** command on your device.

2.
Find the crypto PKI trustpoint configuration.

3.
In the crypto PKI trustpoint configuration, look for the trustpoint enrollment configuration. If the trustpoint enrollment is configured for "selfsigned," then look for the selfsigned certificate configuration.

Output example:

```
crypto pki trustpoint TP-self-signed-XXXXXXXX
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-662415686
  revocation-check none
  rsakeypair TP-self-signed-662415686
!
!
crypto pki certificate chain TP-self-signed-XXXXXXXX
certificate self-signed 01
  3082032E 31840216 A0030201 02024101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494A531D 53656C66 2D536967 6E65642D 43657274
  ...
  ECA15D69 11970A66 252D34DC 760294A6 D1EA2329 F76EB905 6A5153C9 24F2958F
  D19BFB22 9F89EE23 02D22D9D 2186B1A1 5AD4
```

- **If the trustpoint enrollment is *not* configured for "selfsigned":** The device is not impacted by this field notice. No action is required.
- **If the trustpoint enrollment *is* configured for "selfsigned" *and* if the self-signed certificate appears in the configuration:** The device might be impacted by this field notice. Continue to Step 4.

4.
If you determined in Step 3 that the trustpoint enrollment is configured for "selfsigned" and that the self-signed certificate appears in the configuration, then check to see if the self-signed certificate is applied to a feature on the device.

Various features that might be tied to the SSC are shown in these sample configurations:

- **For HTTPS Server**, this text must be present:

```
ip http secure-server
```

Additionally, a trustpoint may also be defined as shown below. If the command below is not present, the default behavior is to use the self-signed certificate.

```
ip http secure-trustpoint TP-self-signed-XXXXXXXX
```

If a trustpoint is defined and it points to a certificate other than the self-signed certificate, you are not impacted. The impact of the expired certificate is minor because self-signed certificates are already untrusted by web browsers and generate a warning even when they are not expired. The presence of an expired certificate may change the warning you receive in the browser.

- **For SIP over TLS**, this text will be present in the configuration file:

```
voice service voip
sip
  session transport tcp tls
!
sip-ua
crypto signaling default trustpoint <self-signed-trustpoint-name>
! or
crypto signaling remote-addr a.b.c.d /nn trustpoint <self-signed-trustpoint-name>
!
```

- **For Cisco Unified CME with encrypted signaling enabled**, this text will be present in the configuration file:

```
telephony-service
 secure-signaling trustpoint <self-signed-trustpoint-name>
 tftp-server-credentials trustpoint <self-signed-trustpoint-name>
```

- **For Cisco Unified SRST with encrypted signaling enabled**, this text will be present in the configuration file:

```
credentials
 trustpoint <self-signed-trustpoint-name>
```

- **For Cisco IOS dspfarm resources (Conference, Media Termination Point, or Transcoding) with encrypted signaling enabled**, this text will be present in the configuration file:

```
dspfarm profile 1 conference security
trustpoint <self-signed-trustpoint-name>
!
dspfarm profile 2 mtp security
trustpoint <self-signed-trustpoint-name>
!
dspfarm profile 3 transcode security
 trustpoint <self-signed-trustpoint-name>
!
sccp ccm 127.0.0.1 identifier 1 priority 1 version 7.0 trustpoint <self-signed-trustpoint-name>
!
```

- **For STCAPP ports configured with encrypted signaling**, this text will be present in the configuration file:

```
stcapp security trustpoint <self-signed-trustpoint-name>
stcapp security mode encrypted
```

- **For Cisco Unified Communications Gateway Services API in Secure Mode**, this text will be present in the configuration file:

```
uc secure-wsapi
ip http secure-server
ip http secure-trustpoint TP-self-signed-XXXXXXXX
```

- **For SSLVPN on Cisco IOS**, this text will be present in the configuration file:

```
webvpn gateway <gw name>
 ssl trustpoint TP-self-signed-XXXXXXXX
```

- **For SSLVPN on Cisco IOS XE**, this text will be present in the configuration file:

```
crypto ssl policy <policy-name>
 pki trustpoint <trustpoint-name> sign
```

- **For IKEv2**, the self-signed certificate is used if this configuration is present:

```
crypto ikev2 profile <prof name>
 authentication local rsa-sig
 pki trustpoint TP-self-signed-xxxxxx
```

- **For ISAKMP (IKEv1)**, the self-signed certificate is used if this configuration is present:

```
crypto isakmp profile <prof name>
 ca trust-point TP-self-signed-xxxxxx
```

Note: Any ISAKMP policy that does not specify an authentication method (see the example below) will also use the SSC.

```
crypto isakmp policy <number>
 encryption aes
 hash sha
 group 5
 lifetime 84400
!
```

- **For SSH Server**, this text will be present in the configuration file:

```
ip ssh server certificate profile
 ! Certificate used by server
 server
  trustpoint sign TP-self-signed-xxxxxx
```

> **Note:** You may notice the self-signed certificate truststore name shown in the output of the **show ip ssh** CLI command. This is *NOT* an indication that you are exposed to the issue described in this Field Notice. If you only log into a device with a username / password or by use of an RSA key pair, you are *NOT* affected by this Field Notice.

- **For RESTCONF**, this text will be present in the configuration file:

```
restconf
 ip http secure-trustpoint TP-self-signed-XXXXXXXXX
! OR
 ip http client secure-trustpoint TP-self-signed-XXXXXXXX
```

- **For WAAS**, there is no specific configuration file text to identify. The trustpoint configuration and SSC configuration that are described in steps 1 - 3 above are sufficient. The device is affected if it runs Cisco IOS XE and is configured with an SSC (as described in steps 1 - 3 above) that expires on 2020-01-01 00:00:00 UTC.

> **Note**: Existing WAAS deployments are not affected by an expired SSC. However, new WAAS Appnav-XE (Cisco IOS XE) devices cannot be registered after the SSC expires. The SSC validity is only checked when WAAS registers a new Appnav-XE device to the WAAS Central Manager (CM).

Additional Information

For additional technical details, refer to IOS Self-Signed Certificate Expiration on Jan. 1, 2020.

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
- By 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.

Quick Links

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap