Updates to the Cipher Suites in Secure Syslog

draft-ciphersuites-in-sec-syslog-00

Chris Lonvick, **Joe Salowey**, Sean Turner

SECDISPATCH@IETF113 — 20220322

What’s the problem?

IEC 62351 TC 57 WG15 wanted to refer to syslog but RFC 5425 pins to TLS 1.2 and the MTI algorithm at the time, which was TLS_RSA_WITH_AES_128_CBC_SHA and is now deprecated.

What can we do about it?

Nothing: IEC TC 57 WG15 offered to incorporate and update the algorithms.

Maintain our RFCs: Produce an I-D to update the syslog+TLS and syslog+DTLS algorithms.

What’s in the I-D?

Justification for the change.

Updates to RFC 5425 (syslog+TLS) & RFC 6012 (syslog+DTLS):

- **MUST:** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- **MAY:** (D)TLS 1.3
  - **NEED:** 0-RTT recommendation

A lengthy author’s note, which will be removed prior to publication, that explains diffs from -00 to -01 and a note the IEC WG will include in their standard.

How should this be dispatched?

Existing WG?

BOF?

AD Sponsor?

ISE?