Non-TLS Port Deprecation in Alder Lake Generation

Supplemental Guidance

November'2022

intel®

Non-TLS Port Deprecation in Alder Lake Generation

Background:

- As defined by **new** RCR 14016948484, Intel is backporting the deprecation of non-TLS ports (16992) in Intel® 12th Generation Alder Lake platforms. This change requires an upgraded CSME firmware and the use of updated Intel® EMA tools to aid adoption.
- This change impacts both Client/Commercial Alder Lake (ADL) 16.0 platforms as well as Server/Workstation Intel® Xeon Platforms running CSME firmware 16.10.
- The original deprecation of non-TLS support was implemented in 13th Generation Raptor Lake platforms. Early communication of this change was provided to OEM partners in Q1'2021 via advisory: 621534
- With 13th Gen Raptor Lake added to the roadmap as a drop-in/cross-shipping refresh platform to Alder Lake systems, some concerns were raised about functional parity for designs that ship with CSME 16.0 firmware and use non-TLS ports (16992) while the refresh CSME 16.1 systems rely on TLS-only port (16993) support.

Impact:

- For in-field systems provisioned with non-TLS ecosystem, performing the FW update will automatically disable non-TLS network ports and re-generate a self-signed cert from the Certificate Authority built into CSME. Remote connectivity will be lost until reconfigured for access using TLS-only ports.
- Intel® EMA version 1.8.0 is a minimum required version to use use with all impacted systems. Software package released WW31'22, see details at Intel Download Center
    - For Desktop/Workstation ecosystems require an additional fix with Intel® EMA to resolve TLS certificate issue. Intel® EMA 1.9.0 will have include this fix with a target release WW47'22

Non-TLS Port Deprecation in Alder Lake Generation

Mitigation:

- For Server/Workstation 16.10 designs, firmware changes are provided ahead of PV milestone release WW45’22
- For Alder Lake Client/Commercial designs, firmware changes are provided at MR3 BKC release as of WW40’22
  - Minor FW version shall update to 16.1 and align with Raptor Lake compatibility

Mitigation Details:

- No re-provisioning of AMT/ISM service is required. The user will be prompted to accept the newly generated self-signed cert (to establish the trusted CA). In order to confirm the console communicates with a real AMT machine, Intel recommends using the AMT-Authenticate API.
- Remotely managed systems will need to reconfigure the connection settings they use with their remote manageability tools to migrate support to secure TLS connection.
  - Example: With Intel® EME, user would modify the network configuration to update from non-TLS configuration (HTTP; 16992) to new secure TLS configuration (HTTPS; 16993).
  - Please see appendix for specific port closure details

See details on the SDK page:

Using a self-signed certificate allows the developer to initially enable a TLS connection with untrusted self-signed certificates. When moving towards productization, the developer should switch to use certificates provided by a trusted certificate authority. In absence of deployment of a trusted certificate authority, the WSMAN AMTAuthenticate() command must be used to verify that the endpoint is authentic Intel AMT Firmware.

Appendix

Non-TLS Port Deprecation Support Change Overview

Before

Intel® AMT/ISM includes support for TCP and TLS remote ports

Port	Use	Local	Remote	CIRA
16992	SOAP over TCP	Yes	Yes	Yes
16993	SOAP over TLS	Yes	Yes	Yes
16994	Redirection over TCP	No	Yes	Yes
16995	Redirection over TLS	No	Yes	Yes
623	DASH over TCP	Yes	Yes	Yes
664	DASH over TLS	Yes	Yes	Yes
5900	VNC (Virtual Network Computing) - remote control program	No	Yes	Yes

After

Intel® AMT/ISM shall support only HTTPS\TLS for the remote ports(16993, 16995, 664), and will not open HTTP\TCP ports (16992, 16994, 623)

Port	Use	Local	Remote	CIRA
16992	SOAP over TCP	Yes	No	Yes
16993	SOAP over TLS	Yes	Yes	Yes
16994	Redirection over TCP	No	No	Yes
16995	Redirection over TLS	No	Yes	Yes
623	DASH over TCP	Yes	No	Yes
664	DASH over TLS	Yes	Yes	Yes
5900	VNC (Virtual Network Computing) - remote control program	No	No (To be Removed as separate RCR and delivered in same FW)	Yes


intel