CODRA **Security Bulletin**

☒ Panorama COM
☒ Panorama E²
☒ Panorama H²
☐ Panorama P²
☐ Panorama SLP
☐ Autre

Reference	Pano/BS-011-EN
Title	Hardening of the TLS configuration for Panorama functions accessible via HTTPS
Issue date	June the 7th 2019
Severity	Standard
Document version	1.1
Source(s)	External Security Audit

Hardening of the TLS configuration for Panorama functions accessible via HTTPS

1 Description

Several Panorama features can expose an HTTPS server to their client:

- **The OPC-UA data server**: An HTTPS server is exposed if, for a Panorama E² or COM functional server, an "OPC-UA Server" object has been added in the System unit and configured:
  - With the *Scheme* property set to "https Schema"
  - Or with a "Access Point" child-object whose *URL* property starts with "https://"
- **The Historian OPC-UA-HA server**: An HTTPS server is exposed if the configuration file "%ProgramData%/Codra/Panorama/PanoITService.exe.config" has been modified to add, under the node "PanoITWebService/Database", an entry of the type: `<add key="UA_HTTPS_BINDING" value="https://..."></add>`
- **The mobile HMI server**: An HTTPS server is exposed if the *URL* property of the object "Mobile HMI server" starts with "https://"
- **SigFox and LoRa acquisition (from Panorama Suite 2019)**: An HTTPS server is exposed if, on a "SigFox Connection" or "LoRa Connection" object, the *UseNotification* property is set to *True* and the *LocalUrl* property starts with " https://».

In order to harden the default configuration of Windows and reduce the risk of attacks on HTTPS servers exposed by Panorama, you must:

- Limit supported TLS protocol versions

- Limit supported cypher suites

Warning: This operation may result in incompatibilities with clients or servers that do not support the latest versions of TLS or the strongest cypher suites.

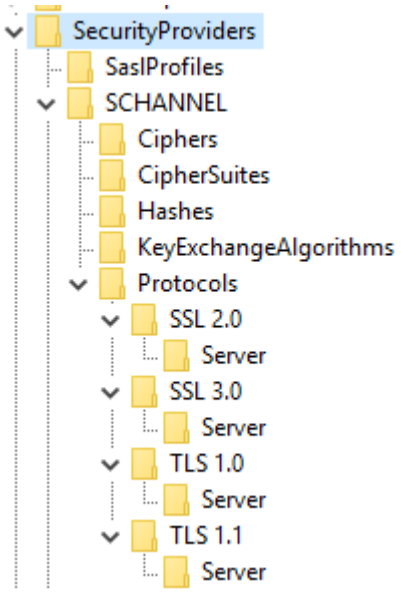
Affected versions
• All version of Panorama Suite

2 Solution

2.1 Limit supported versions of the TLS protocol

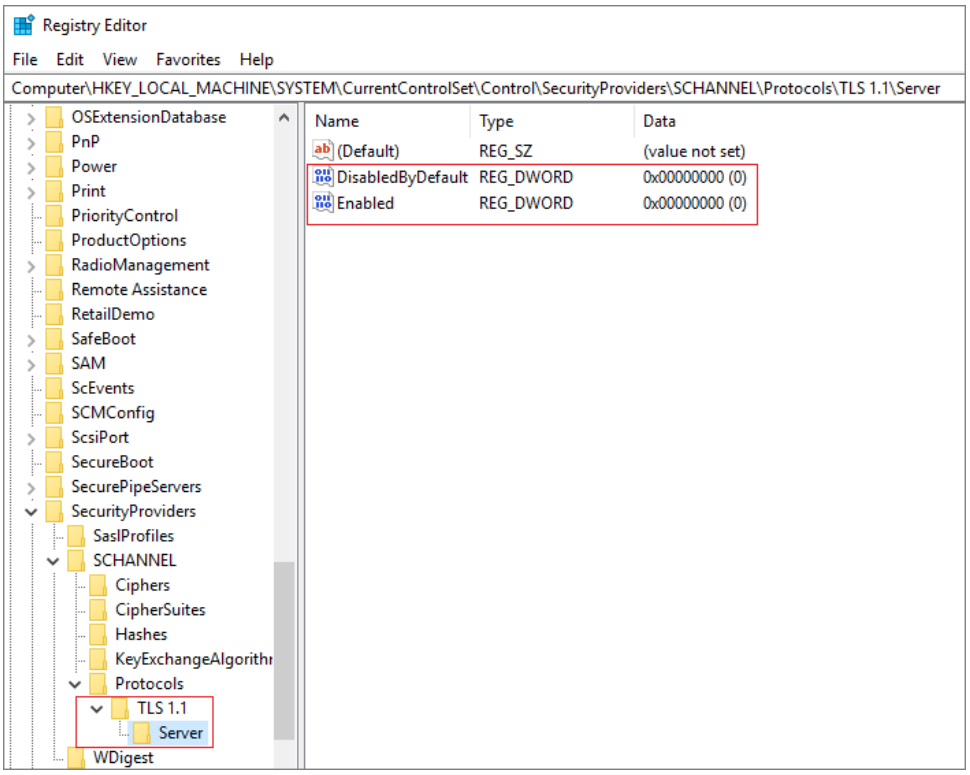
The choice of TLS protocol versions supported by the server is made from the registry of the server.

1. Open the Registry Editor as Administrator
2. Select the node:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
3. If the following nodes do not exist, create them:
   - « SSL 2.0/Server »
   - « SSL 3.0/Server »
   - « TLS 1.0/Server »
   - « TLS 1.1/Server »



4. Under each of the "Server" nodes, create the following DWORD type keys:
   - "Enabled" with the value "0"
   - "DisabledByDefault" with the value "0"

The following capture shows the disabling of version 1.1 of TLS:



5. Restart the machine

Once this configuration is completed, the server only allows the connection of clients in TLS version 1.2 and higher.

2.2 Limit supported cypher suites

Cypher Suite selection

The choice of cypher suites supported by the server is made from the "gpedit.msc" Group Policy Editor of the server.

You need to modify the following parameter:

- Parameter name: *Computer Configuration> Administrative Templates> Network> SSL Configuration Settings> SSL Cipher Suite Order*
- Value: *Enabled*
- Options:
  - SSL Cipher suites:
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256

Then restart the machine.

Note: When the machine is registered in a domain, this configuration can be performed at the Active Directory Group Policy level that applies to that machine.

Connectivity of TLS clients hosted by the server

If, in addition of a TLS server, the machine hosts a TLS client, then cypher suites limitation can impact client connectivity. For example, it's the case when the machine is a functional server with OPC-UA data server (a TLS server) with OPC-UA acquisition via HTTPS (a TLS client).

The solution depends on the kind of clients TLS:

- *OPC-UA acquisition client, SigFox or Objenious IoT acquisition, Mobile HMI server with alarm notification*: the following .REG file sets the needed values in registry:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\
v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\
v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

- *SQL Client of a server requiring SQL encryption*: « Microsoft SQL Server 2012 Native Client » must be updated to version 11.4.7001.0 or higher.

3 History

Version 1.1	June 7th 2019	Initial version