CODRA **Security Bulletin**

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

Reference	Pano/BS-010-EN
Title	Failure to authenticate Panorama OPC-UA server HTTPS clients and add access control based on a list of thumbprints
Issue date	May the 27th 2019
Severity	High
Document version	1.1
Source(s)	External Security Audit

Failure to authenticate Panorama OPC-UA server HTTPS clients and add access control based on a list of thumbprints

1 Description

If the Panorama OPC-UA server function is **enabled** and **usable through HTTPS**, then it is possible for an attacking client, located on the same network as the server, to connect to the server without being authenticated and to bypass the access control, despite the security configuration of the server requiring authentication.

It is the case:

- If for a Panorama E² or COM functional server, an "OPC-UA Server" object has been added in the System unit and configured:
  - Either with the Scheme property set to "https Schema"
  - Or with a child-object "Access Point" whose URL property starting with "https://"
- If for a Panorama H² server, 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>`

Affected versions
• All version of Panorama Suite

2 Solution

Install the following updates:
- For Panorama Suite PS 2017: PS2-1700-03-2128 or higher
- For Panorama Suite PS 2019: PS2-1800-23-1157 or higher

On all machines where an OPC-UA Panorama server is activated and uses HTTPS.

This update provides:
- A correction to take into account the security configuration of the OPC-UA server in HTTPS as set in the configuration file.
- An evolution of the OPC-UA data server of the E² or COM functional server which introduces a new type of access control based on the client certificate thumbprint (This evolution is not available for the OPC-UA-HA server of the Historian server).

2.1 Taking into account the security configuration

Starting from update PS2-1700-03-2128 or PS2-1800-23-1157, an OPC-UA server accessible in HTTPS supports only the strongest security mode among those configured on the server ("Authentication and encryption "," Authentication "," Not secure ").

The security configuration is described in detail in the Panorama manual:
- For a E² or COM functional server, see:
  The Data Server Function > The OPC UA server > Using the Composer OPC UA Server > Configuring the Composer OPC UA server
- For an Historian server, see:
  The Historian server > Configuring the Historian Web service

2.2 Access control based on the client certificate thumbprint

Starting from update PS2-1700-03-2128 or PS2-1800-23-1157, it is possible to setup an access control based on a list of client certificate thumbprints authorized to connect to the OPC-UA data server.
This thumbprint list is defined in the Panorama application.

The benefits of this type of access control are as follows:
- It allows access control based only on a TLS (HTTPS) certificate, avoiding the use of an OPC-UA application certificate.
- It avoids having to finely manage trusted TLS certificates in the Windows store (because the store can be updated automatically by the operating system).
- It makes it possible to manage the access policy directly in the Panorama application, and thus facilitate the operations of distributing the access policy from one server to another.

As soon as this list is configured, all the certificates presented by a client (TLS certificate and OPC-UA application certificate) must be in this list for the connection to be authorized.
This is the recommended configuration for the Panorama Suite OPC-UA Data Server.

3 History

Version 1.1	May 27th 2019	Initial version