CODRA **Security Bulletin**

- ☒ Panorama COM
- ☒ Panorama E²
- ☐ Panorama H²
- ☐ Panorama P²
- ☐ Panorama SLP
- ☐ Other

Reference	Pano/BS-009-EN
Title	Limit interfaces listened by the OPC-UA server of Panorama
Issue date	Apr the 24th 2019
Severity	Minor
Document version	1.1
Source(s)	External Security Audit

Limit interfaces listened by the OPC-UA server of Panorama

1 Description

By default, OPC-UA clients can connect from all network interfaces of a functional server to use the "OPC-UA Data Server" function.
In order to strengthen station configuration, ports usable to establish a connection with the server must be limited to the network interface dedicated to communication with the OPC-UA clients.

Affected versions
• All version of Panorama Suite

2 Solution

The solution varies according to the schema type defined in the configuration of the "OPC-UA Server" object (HTTP, HTTPS, OPC.TCP or NET.TCP).

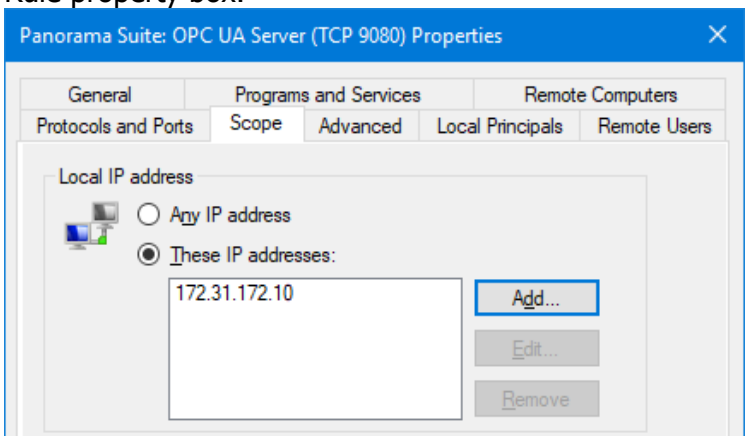
2.1 HTTP or HTTPS scheme

The Panorama manual describes how to allow incoming HTTP and HTTPS connections to the OPC-UA data server port using a Windows Firewall rule.

As a reminder, this rule is created by the Network and Security tool and described in the following chapter of the manual:
Application security > Security and operation on a network > Configuration for using Panorama on a network > Configuring the firewall of Panorama machines > Windows "standard" firewall configuration > Authorizing inbound flows > Adding an exception for Web services

The solution is to **complete this rule** to allow incoming connections only on the local address of the network interface dedicated to communication with OPC-UA clients.

This is done by adding the local IP address in the "Scope" tab of the Windows Firewall Rule property box.



2.2 OPC.TCP or NET.TCP scheme

The Panorama manual describes how to allow incoming connections for the Panorama Composer process through a Windows Firewall rule.

As a reminder, this rule is created by the Network and Security tool and described in the following chapter of the manual:
Application security > Security and operation on a network > Configuration for using Panorama on a network > Configuring the firewall of Panorama machines > Windows "standard" firewall configuration > Authorizing inbound flows > Adding an exception for the applications

The solution is to **create a new rule** to complement this rule.

This rule must BLOCK incoming connections to the Panorama Composer.exe process, for the TCP protocol and the OPC-UA server listening port from all local addresses that do not match the network interface dedicated to communication with clients.

3 History

Version 1.1	Apr the 24th 2019	Initial version