Codra **Security Bulletin**

1☒ Panorama COM
☒ Panorama E²
☒ Panorama HISTORIAN
☐ Panorama P²
☐ Panorama SLP
☐ Other

Reference	Pano/BS-006-EN
Title	OPC UA security vulnerabilities
Issue date	26 - Oct - 2018
Severity	High
Document version	1.1
Source(s)	https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2018-12086.pdf https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2018-12585.pdf

OPC UA security vulnerabilities on server

1 Description

1.1 Potential stack overflow by sending malicious queries to server

If the OPC-UA server function has been activated:
- for a Panorama functional server, by adding a “OPC UA Server” in the application,
- for the Panorama Historian server, if the default configuration has not been changed,

then an attacking client can trigger a stack overflow in OPC UA server by sending malicious queries, causing the Panorama functional server or the Panorama Historian server to stop.

The criticality is rated 7.5 on the CVSS v3.0 scale. The criticality of this flaw is high because an attacker can cause unavailability of the target server from the network.

Affected versions
• Panorama Suite 2017 without an update of family 03 ≥ PS2-1700-03-1257 • Panorama Suite 2019 is not concerned

1.2 Potential denial of service attack from a Panorama server, which is attacker-induced

If the OPC-UA server function has been activated:

- for a Panorama functional server, by adding a “OPC UA Server” in the application,
- for the Panorama Historian server, if the default configuration has not been changed,

then, an attacker can, by sending malicious queries, cause the Panorama functional server or the Panorama Historian server querying another server, causing a denial of service attack on that other server.

Criticality is rated 8.2 on the CVSS v3.0 scale.

Affected versions
• Panorama Suite 2017 without an update of family 03 ≥ PS2-1700-03-1257 • Panorama Suite 2019 is not concerned

2 Solution

Installing update PS2-1700-03-1257 or newer on machines using a Panorama functional server with an OPC UA Server object, or a Panorama Historian server, with the OPC-UA server function enabled.

If the OPC-UA server function is not used for Historian, it is strongly recommended to disable it by changing the Historian configuration file as follows:

File: %ProgramData%\Codra\Panorama\PanoITConfig.xml

Section <Database>:

Add the following key:

<add key="UA_ENABLED" value="False"></add>

3 History

Version 1.0	14 - Sept - 2018	Initial version
Version 1.1	26 - Oct - 2018	Updated affected versions