Codra Security Bulletin

- [x] Panorama COM
- [x] Panorama E²
- [ ] Panorama HISTORIAN
- [ ] Panorama P²
- [ ] Panorama SLP
- [ ] Other

Reference	Pano/BS-005-EN
Title	OPC binding Basic128Rsa15 is deprecated
Issue date	26 - Oct - 2018
Severity	Standard
Document version	1.2
Source(s)	https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2018-7559.pdf

OPC binding Basic128Rsa15 is deprecated

1 Description

OPC UA Basic128Rsa15 cryptosuite relies on cryptographic algorithms that are not strong enough today to ensure privacy on encrypted communications between an OPC UA client and its server.

It is therefore recommended to stop using this cryptosuite on UA bindings, and to use Basic256 and Basic256Sha256 instead.

The default binding configuration in Panorama uses Basic128Rsa15, it is therefore required to modify the OPC UA clients and server configuration in the Panorama application to use better security options. This default configuration will be described as unsafe in future Panorama versions, but will be kept for compatibility with older servers.

Affected versions
• All Panorama Suite versions

2 Solution

On OPC UA client objects in the Panorama application, set the *SecurityPolicy* property either to « Basic256 and Basic256Sha256 », or to « Basic256Sha256 ».

On OPC UA server object in the Panorama application, set the *SecurityPolicy* property either to « Basic256 and Basic256Sha256 », or to « Basic256Sha256 ».

3 History

Version 1.1	13 - Apr - 2018	Initial version
Version 1.2	26 - Oct - 2018	Updated affected versions