Codra **Security Bulletin**

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

| | |
|---|---|
| **Reference** | Pano/BS-003-EN |
| **Title** | Panorama configuration hardening |
| **Issue date** | 26 - Oct - 2018 |
| **Severity** | Low |
| **Document version** | 1.3 |
| **Source(s)** | |

# Panorama configuration hardening

## 1 Description

This security update provides complements to the Panorama security recommendations in the Panorama Suite manual:

- Changing the Archive Server service ***PnArchiveServer*** execution account and impact on the local archive directory rights policy.
- Changing the External Directory Management service ***PnUserInfo*** execution account.
- Changing the SNMPv3 Traps Reception service ***MG-SOFT SNMP Trap Service*** execution account.
- Disabling the ***Composer*** service on workstations that do not host a functional server.
- Limiting the ***SNMP Traps*** listening interface.
- Disabling incoming connection listening for ***Modbus***.

## 2 Solution

### 2.1.1 Changing the Archive Server service *PnArchiveServer* execution account

By default, the Archive Server service *PnArchiveServer* runs in the "System" account.
In a context requiring system hardening, this service must run in the non-privileged "Network Service" account.

**Warning**:

- This configuration is only possible from Windows 10 and Windows Server 2016.

- Changing the *PnArchiveServer* service account requires checking the access rights to all archive directories. The "Network Service" account must have the "Modify" permission.

| **Affected versions** |
| --- |
| • Panorama Suite 2017<br>• Panorama Suite 2019 is not concerned |

### 2.1.2 Changing the External Directory Management service *PnUserInfo* execution account

By default, the External Directory Management service *PnUserInfo* runs in the "System" account.

In a context requiring system hardening, this service must run in the non-privileged "Local Service" account.

| **Affected versions** |
| --- |
| • Panorama Suite 2017<br>• Panorama Suite 2019 is not concerned |

### 2.1.3 Changing the SNMPv3 Traps Reception service *MG-SOFT SNMP Trap Service* execution account

By default, the SNMPv3 Traps Reception service *MG-SOFT SNMP Trap Service* runs in the "System" account.

In a context requiring system hardening, this service must run in the non-privileged "Local Service" account, or, if Composer runs in a non-privileged account, in the same account than Composer.

Moreover, the service must be set to “Automatic” startup type.

The selected account must have additional rights on the following registry keys:

- *HKEY_LOCAL_MACHINE\SOFTWARE\MG-SOFT\WinSNMP*
- *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MG-SOFT\WinSNMP*

To do this, open the “regedit’ tool using administrative rights, navigate to the registry key to configure, and select the “Permissions…” item in the context menu. Add the service account and grant it the “Full Control” permission.

| **Affected versions** |
| --- |
| • Panorama Suite 2017<br>• Panorama Suite 2019 (the user manual has been updated) |

### 2.1.4 Disabling the *Composer* service

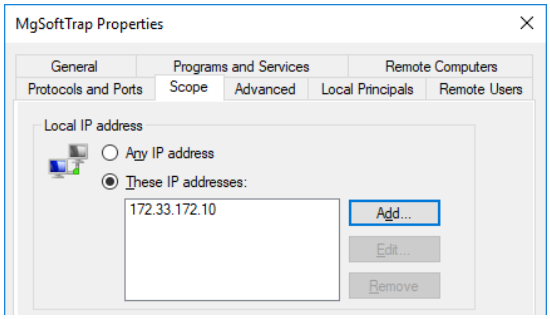
By default, the ***Composer*** service runs in the "System" account of the machine.

In a context requiring system hardening, on workstations that do not host a functional server, the ***Composer*** service must be disabled using its properties dialog box in the Windows Services Control Panel.

| Affected versions |
|---|
| • Panorama Suite 2017<br>• Panorama Suite 2019 |

### 2.1.5 Limiting the *SNMP Traps* listening interface

By default, ***SNMP Traps*** can be received on all network interfaces of a functional server using the “SNMP Manager” function.
In a context requiring system hardening, incoming connections on the ***Traps*** listening port must be limited to the network interface dedicated to the communication with the SNMP agents.
To do this, the Windows Firewall exception allowing incoming connections on the process “C:\Windows\System32\snmptrap.exe” (and “MgWTrap3.exe” if SNMPv3 is used) should only apply on the local address of the network interface dedicated to the communication with the SNMP agents.
This is done by adding the IP address in the “Scope” tab of the Windows Firewall exception properties page.




| Affected versions |
|---|
| • Panorama Suite 2017<br>• Panorama Suite 2019 |

### *2.1.6* Disabling incoming connection listening for *Modbus*

The « Modbus Data Acquisition » function listens the port 502 on all network interfaces.
To prevent this unnecessary action, install update PS2-1700-18-1157 or higher.

| Affected versions |
|---|
| • Panorama Suite 2017 without an update of family 18 ≥ PS2-1700-18-1157<br>• Panorama Suite 2019 is not concerned |

# 3 History

| | | |
|---|---|---|
| Version 1.1 | 17 - Apr - 2018 | Initial version |
| Version 1.2 | 19 - June - 2018 | Changing the SNMPv3 Traps Reception service execution account<br>Limiting the *SNMP Traps* listening interface<br>Disabling incoming connection listening for *Modbus* |
| Version 1.3 | 26 - Oct - 2018 | Updated affected versions |