tyco

PRODUCT SECURITY ADVISORY (UPDATE)

28-March-2019 CPP-PSA-2019-01 v2

Tyco security solutions has confirmed a vulnerability in the exacqVision Enterprise System Manager (ESM) v5.12.2 (and prior) application. In the impacted versions, an unauthorized user could potentially exploit this vulnerability to achieve unauthorized privilege escalation can be achieved. This advisory provides guidance on mitigation actions to avoid a potential exploit.

Scope: This vulnerability impacts exacqVision ESM v5.12.2 and all prior versions of ESM running on a Windows operating system (except Windows Server). This issue does not impact Linux deployments with permissions that are not inherited from the root directory.

Mitigation:
The following mitigating steps are recommended for Windows 10 Desktop OS. Other versions of Windows may have different nomenclature, but the same mitigating steps are recommended.

Step 1: Launch a command prompt with Administrator privileges, then run the following 4 commands sequentially:

```
cacls C:\exacqVisionESM /e /R "Authenticated Users"
cacls C:\exacqVisionESM\uninstall.exe /e /R "Authenticated Users"
cacls C:\exacqVisionESM\EnterpriseSystemManager /e /T /R "Authenticated Users"
cacls C:\exacqVisionESM\apache_solr /e /T /R "Authenticated Users"
```

Step 2: Open the 'Services' applet and restart all of the following:

ESMImporter
ESMDatarolloff
ESMSendemail
ESMWebservice
solrJetty
solrApache

Fix:
Tyco security solutions is working on a fix that will be incorporated into a future version of the exacqVision ESM that will not require execution of the foregoing manual mitigation process.

References:
Please visit the Tyco security solutions, Cyber Protection website to register for and download security advisories.

Sincerely,
Product Security Team

Johnson Controls