Solr vulnerability - CVE-2017-12629

Enterprise Manager

Enterprise Manager (formerly ESM) includes a version of Apache Solr which is vulnerable to attack allowing remote code execution. Further information can be found here: https://nvd.nist.gov/vuln/detail/CVE-2017-12629

Mitigation: It is recommended that you follow the steps below appropriate for your Operating System.

For Windows

Note: File paths vary depending on installation, 64-bit or 32-bit.

1. Launch services, then stop 'solrJetty'
2. Click the 'Start' button and type 'Notepad.exe'. Right-click notepad and select 'Run as administrator'.
3. Click 'File', then 'Open', and navigate to the following file based on your install location:
    - For 64-bit:"C:\exacqVisionESM\apache_solr\apache-solr\server\solr\collection1\conf\solrconfig.xml"
    - For 32-bit:"C:\exacqVisionESM\apache_solr\apache-solr\solr\collection1\conf\solrconfig.xml"
4. Add the following highlighted section just above the "Function Parsers" line:

```
  -->
<!-- example of registering a query parser -->
<!--
  <queryParser name="myparser" class="com.mycompany.MyQParserPlugin"/>
  -->
  <queryParser name="xmlparser" class="solr.ExtendedDismaxQParserPlugin"/>
<!-- Function Parsers
    http://wiki.apache.org/solr/FunctionQuery
```

5. If 64-bit, click 'File', then 'Open', and navigate to the following file: "C:\exacqVisionESM\apache_solr\apache-solr\bin\solr.cmd"
    - Find the line: set START_OPTS=%START_OPTS% !GC_TUNE! %GC_LOG_OPTS%
    - Below this line, add the following: set "START_OPTS=%START_OPTS% -Ddisable.configEdit=%true%"
6. Save the file.

Created On: 2nd February 2021
KB Number: KB-00032-32-210202

7. Click 'File', then 'Open', and navigate to the following file based on your install location:
    - For 64-bit: Launch 'regedit' from start menu.
        i. Go to HKEY_LOCAL_MACHINE->SYSTEM->ControlSet001->Services->solrJetty
        ii. Double click ImagePath
        iii. In value data put double quotes around C:\PROGRA~1\EXACQV~1\ENTERP~1\apache_solr/apache-solr\scripts\prunsrv.exe
    - For 32-bit: "C:\exacqVisionESM\apache_solr\apache-solr\scripts\serviceinstall.bat"
        i. Find the entry: ++JvmOptions=-XX:MaxPermSize=128M
        ii. Add a space after this entry and add: ++JvmOptions=-Ddisable.configEdit=true
        iii. Fine the quoted text: --Install="C:\exacqVisionEsm\apache_solr/apache-solr\scripts\prunsrv.exe\"
        iv. Replace it with: --Install="'C:\exacqVisionEsm\apache_solr/apache-solr\scripts\prunsrv.exe\'"

Note: Ensure there is a space after this entry.

8. Save the file and close Notepad.
9. Click the Windows 'Start' button and type 'cmd'. Right-click on "Command Prompt' and select 'Run as administrator'.
10. Run the following two commands sequentially:

    C:\exacqVisionEsm\apache_solr\apache-solr\scripts\serviceinstall.bat

    C:\exacqVisionEsm\apache_solr\apache-solr\scripts\serviceinstall.bat INSTALL

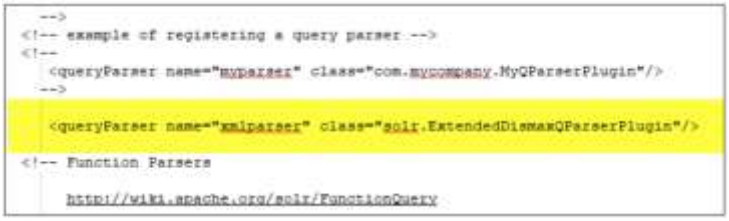
11. Launch services, then start 'solrJetty'

For Linux

Note: File paths vary depending on installation, 64-bit or 32-bit.

1. Open a Terminal.
2. Stop ESMWebservice with the following command:
   sudo /usr/local/exacq/esm/scripts/ESMWebservice stop
   Enter your password and press "Enter"
3. Open 'gedit' (or your preferred text editor) with 'sudo' privileges with the following command: sudo gedit
4. Click 'File', then 'Open', and navigate to the following file based on your install location:
   For 64bit: "/usr/local/exacq/esm/apache_solr/apache-solr/server/solr/collection1/conf/solrconfig.xml"

   For 32bit: "/usr/local/exacq/esm/apache_solr/apache-solr/solr/collection1/conf/solrconfig.xml"
5. Add the following highlighted section just above the "Function Parsers" line:



6. Save the file.
7. Click 'File', then 'Open', and navigate to the following file based on your install location:

   For 64-bit: "/usr/local/exacq/esm/apache_solr/apache-solr/bin/solr"
   Before the line that reads: SOLR_START_OPTS
   Add the line: DISABLE_CONFIG_EDIT="true"

   For 32-bit: "/usr/local/exacq/esm/apache_solr/apache-solr/scripts/ctl.sh"
   After the line: SOLR_PID=""
   Add a new line: DISABLE_CONFIG_EDIT="true"
   Change the line: SOLR=
   To: SOLR="$JAVABIN -Dsolr.solr.home=$SOLR_HOME -Djetty.logs=$INSTALL_PATH/logs/ -Djetty.home=$INSTALL_PATH/ -

jar $INSTALL_PATH/start.jar $INSTALL_PATH/etc/jetty.xml -Ddisable.configEdit=$DISABLE_CONFIG_EDIT"

8. Save the file and close gedit.
9. Back in the terminal, run the following command

   sudo /usr/local/exacq/esm/apache_solr/ctlscript.sh restart

10. Restart ESMWebservice with the following command:

    sudo /usr/local/exacq/esm/scripts/ESMWebservice start