FORUM family CVE-2021-44228 patch

Topic

Instructions to patch products of the FORUM family against the Log4Shell vulnerability (CVE-2021-44228)

Purpose/abstract

This document provides instructions on how to apply the security patch to protect FORUM Archive & Viewer and all related clinical workplaces which are part of the FORUM family. Products and versions listed below are identified to have the vulnerable component. Versions not listed do not contain the component exploited by this vulnerability.

The patch is available for both Windows and a MacOS. An unattended mode is available for automated distribution.

This patch will protect the following products and versions:

- FORUM Archive & Viewer 4.2.x
- Retina Workplace 2.5.x and 2.6.x
- Glaucoma Workplace 3.5.x
- EQ Workplace 1.6 – 1.8
- Cataract Suite 1.3.1
- Advanced Data Export 1.x
- Refractive Workplace 1.0.0
- Laser Treatment Workplace 1.x

Requirements

Parts needed

- FORUM Family Log4j CVE-2021-44228 Patch (FORUM-Family-Log4j-CVE-2021-44228-Patch-x64.exe for Windows or macOS_FORUM-Family-Log4j-CVE-2021-44228-Patch.dmg)

Procedure

Preparation

- Download the FORUM-Family-Log4j-CVE-2021-44228-Patch-x64.exe file from the international website: ZEISS Cyber security - ZEISS Medical Technology | ZEISS International

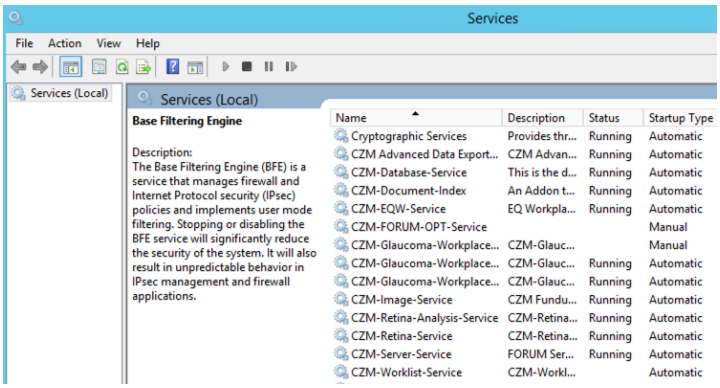
⚠ CAUTION!	**Caution** A new installation or reinstallation of FORUM Viewer or any other FORUM family product will come without the patch described in this document. When the product is uninstalled being in a patched

state, the success/failure indication text file remains in the folder as the product uninstaller is not aware of these files.

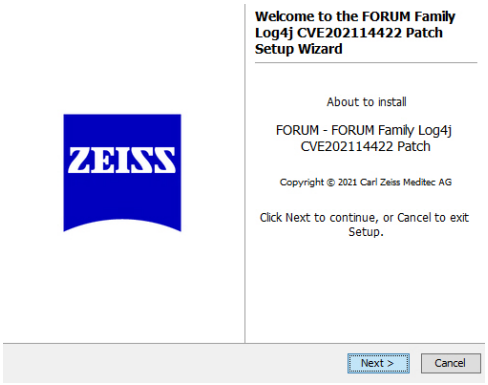
► Ensure the patch is applied after reinstallation unless a new version of the product is available, already containing the fix.

Windows installation

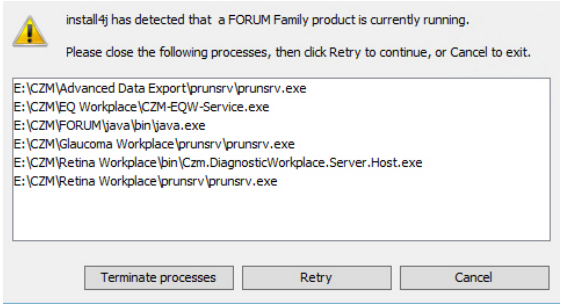
1) Stop all FORUM family products. On the server side, open the Services console and stop all services beginning with CZM-. Close all Applications such as FORUM Viewer, Service Tool, etc.



2) Execute the patch on any computer which may have FORUM Viewer, FORUM Archive or any other of the listed products. Click **Next** to continue.



3) All FORUM family products **currently still running** are displayed. The services should be stopped as described in step one before continuing. Click **Next** to proceed with the patch.



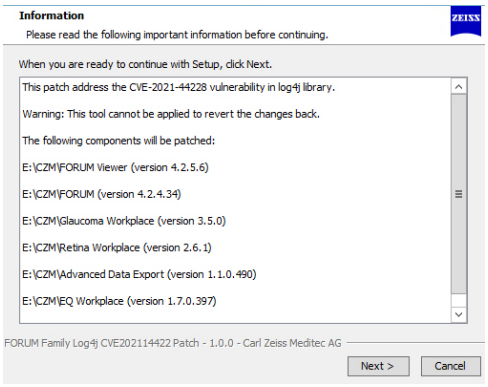
⚠ WARNING!

Warning

All FORUM family products which are still running will be stopped.

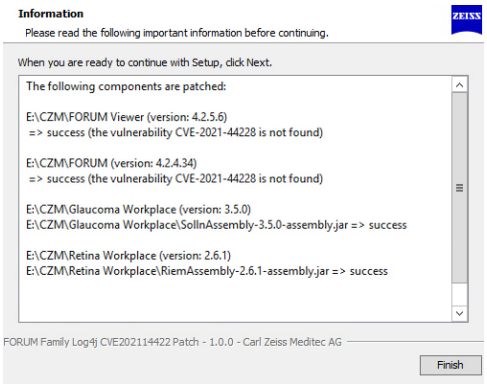
► Gracefully stop all services starting with **CZM-** that are still running. Close all applications such as FORUM Viewer, Service Tool, Tray Icon.

4) All detected products on the system are displayed. The changes performed after clicking **Next** are not reversible. Click Next to patch the system.



5) The results are displayed in summary. Please verify the results. You can run the patch again in case some component was not patched correctly ensuring the services are properly stopped.

6) Click **Finish** to exit the installer.



NOTE

Note

The installer creates a text file within the directory of each product indicating success or failure.

► This is useful to be able to identify the patched / non patched workstations.
Success: Vulnerability-CVE202144228-patched.txt
Failure: Vulnerability-CVE202144228-unpatched-DO-NOT-USE.txt

NOTE

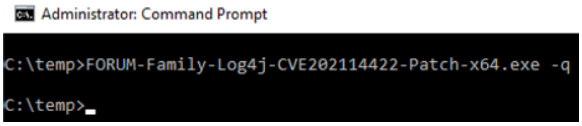
Note

In case some components fail to be patched, the patch can be applied again without causing any harm.

► Run the patch again if not all components were successfully updated.

Windows silent installation

1) Place the patch on a local or on a network location and execute the file using the **-q** (unattended mode) parameter. The patch will be executed without any feedback.



NOTE	**Note** The silent installer is primarily aimed to install the patch on a larger number of FORUM Viewer machines. The install requires administrative privileges on the target computer. ► Placed on a network share, the patch can be executed on remote computers via GPO or other techniques.

NOTE	**Note** The installer creates a text file within the directory of each product indicating success or failure. ► This is useful to be able to identify the patched / non patched workstations.

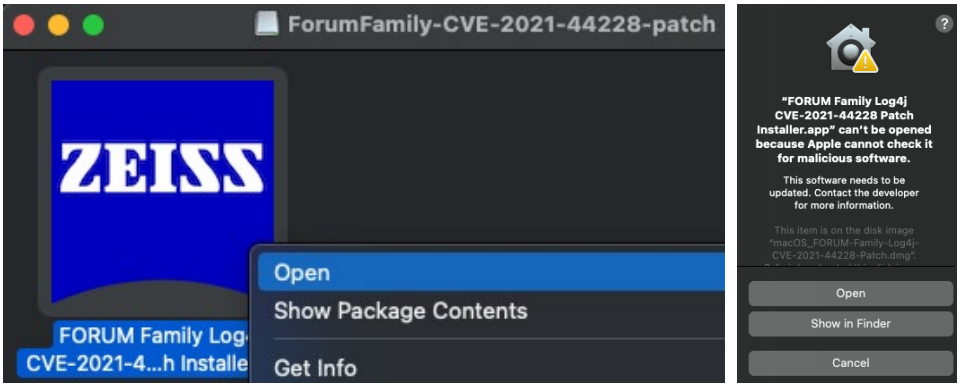
Manual Verification

The vulnerability can be found by manually searching the FORUM family products. The find string (findstr /m /s /i JndiLookup.class .jar) command can be used on Windows systems to search for the JndiLookup.class.

Only if there are no findings returned, the product is not vulnerable to the Log4Shell exploitation. If there are findings, run the patch once again or contact your local ZEISS support representative.

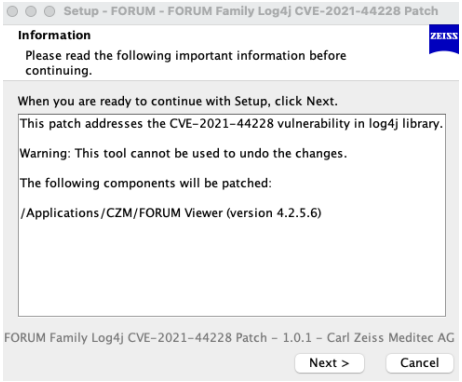
MacOS Installation

1) Quit the FORUM Viewer application.
2) Double-click the downloaded dmg file. Right click the Installer.app when the content of the dmg is presented. Select **Open** and confirm by clicking **Open**.

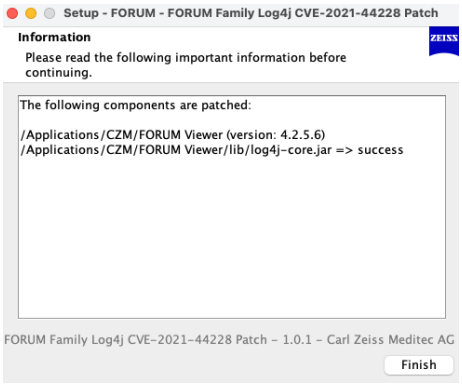


3) Enter the credentials of a user with administrative privileges. Click **Next** on the on the Welcome screen of the patch installer

4) The FORUM Viewer version found is displayed, click **Next** to continue.



5) A confirmation screen is displayed showing that the FORUM Viewer was successfully patched.



6) The Vulnerability-CVE202144228-patched.txt file is placed into the FORUM Viewer installation directory indicating that this installation has been successfully patched.