

Customer Information Bulletin

Figure 4 printers, NextDent 5100, ProJet 6000/7000, ProX 6100, ProX 500, DMP Flex 100, ProX 100/200/300, DMP 320, DMP Flex 350, ProX 800/950, MJP 2500, SLS sPro60, DMP Factory 500

Subject: Log4J Vulnerability – actions to take

Issue:

In response to the discovered Log4J vulnerability (aka CVE-2021-44228 or Log4Shell), we have confirmed that the only 3D Systems product utilizing Log4J is 3D Connect service.

Solution:

The 3D Connect Service adapter code has been updated to the latest Log4J version; and this was pushed automatically to 3D Connect devices on Monday, December 20, 2021. For the update to take effect, customers should restart the affected devices, which include:

- Any 3D Connect adapter PC. You may have this adapter if you own one of the following printers:
 - ProJet 6000 and 7000 SLA
 - ProX 6100 and 500 SLS
 - DMP Flex 100 and ProX 100, 200, and 300 DMP
 - DMP 320 and DMP Flex 350
 - ProX 800 and 950 SLA
 - ProJet MJP 2500
 - sPro60 SLS
 - Factory 500 DMP
- Any machine with 3D Connect built into the hardware:
 - Figure 4 Modular Controller
 - Figure 4 Modular Printers
 - Figure 4 Dental/Standalone/Jewelry Printers



Once the machines have restarted, they will be running the latest version of Log4J, which does not have the vulnerability.

If you have any questions regarding this issue, please reach out to 3D Systems support. They will also be able to confirm that your 3D Connect adapters have been updated to the latest code.

<https://support.3dsystems.com/s/contactsupport>