3D Professional & Production Printers
Customer Information Bulletin

[X] Advisory [ ] Upgrade / Repair / Retrofit [ ] Safety Alert

Subject: **Customer Guidance for WannaCrypt attacks** **For All MJP, CJP, SLA, SLS, DMP Printers**

Problem: Risk of exposure of our printers to the WannaCrypt Ransomware attack

Solution: Detailed instructions for each printer line are included in this CIB as well as links to download the particular update associated with your printer.

At 3D Systems, we are always concerned about the security of our printers, which are based on the Microsoft Windows platform. In general, we do not set our printers to automatically apply Windows Updates or run Anti-Virus/Anti-Malware Software as that can affect the real time processing requirements of our systems. We monitor the Microsoft security updates and from time to time may recommend that our customers update their systems with SPECIFIC Microsoft updates.

While we believe the risk of exposure of our printers to the WannaCrypt Ransomware attack is small, we are encouraging our customers to upgrade their systems using the Microsoft supplied security updates.

Please feel free to contact your local reseller or our Field Support team if you have any questions about this or any issues in performing the update. We include below the contents of the Microsoft Blog with a description of the attack and the information provided by Microsoft, so you may also take appropriate action to update your client Software computers and other computers within your organization.

Customer Information Bulletin

Customer Guidance for WannaCrypt attacks

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
Microsoft solution available to protect additional products

Today many of our customers around the world and the critical systems they depend on were victims of malicious "WannaCrypt" software. Seeing businesses and individuals affected by cyberattacks, such as the ones reported today, was painful. Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers. This blog spells out the steps every individual and business should take to stay protected. Additionally, we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. Customers running Windows 10 were not targeted by the attack today.
Details are below.
In March, we released a security update which addresses the vulnerability that these attacks are exploiting. Those who have Windows Update enabled are protected against attacks on this vulnerability. For those organizations who have not yet applied the security update, we suggest you immediately deploy Microsoft Security Bulletin MS17-010.
For customers using Windows Defender, we released an update earlier today which detects this threat as Ransom:Win32/WannaCrypt. As an additional "defense-in-depth" measure, keep up-to-date anti-malware software installed on your machines. Customers running anti-malware software from any number of security companies can confirm with their provider, that they are protected.
This attack type may evolve over time, so any additional defense-in-depth strategies will provide additional protections. (For example, to further protect against SMBv1 attacks, customers should consider blocking legacy protocols on their networks).
We also know that some of our customers are running versions of Windows that no longer receive mainstream support. That means those customers will not have received the above mentioned Security Update released in March. Given the potential impact to customers and their businesses, we made the decision to make the Security Update for platforms in custom support only, Windows XP, Windows 8, and Windows Server 2003, broadly available for download (see links below).
Customers who are running supported versions of the operating system (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows 10, Windows Server 2012 R2, Windows Server 2016) will have received the security update MS17-010 in March. If customers have automatic updates enabled or have installed the update, they are protected. For other customers, we encourage them to install the update as soon as possible.
This decision was made based on an assessment of this situation, with the principle of protecting our customer ecosystem overall, firmly in mind.
Some of the observed attacks use common phishing tactics including malicious attachments. Customers should use vigilance when opening documents from untrusted or unknown sources. For Office 365 customers we are continually monitoring and updating to protect against these kinds of threats including Ransom:Win32/WannaCrypt. More information on the malware itself is available from the Microsoft Malware Protection Center on the Windows Security blog. For those new to the Microsoft Malware Protection Center, this is a technical discussion focused on providing the IT Security Professional with information to help further protect systems.
We are working with customers to provide additional assistance as this situation evolves, and will update this blog with details as appropriate.
Phillip Misner, Principal Security Group Manager Microsoft Security Response Center

3D Production Printers
Customer Information Bulletin

NOTE: ProJet CJP printers and ProJet 1200 are not affected by the WannaCrypt Ransomware attack, no action is required for these printers.

Instructions and download links for each Printer line are included below:

SLA

ProX 800/950:

- **Windows 7 Standard:**
  1. Download Window 7 Standard patch date zip file
  2. Unzip patch folder and download to USB stick
  3. Insert USB stick into machine
  4. Copy the patch folder to the desktop
  5. Open the folder
  6. Double click on the Win7 Standard Patch x86.bat
  7. Restart machine

ProJet 6000/7000:

- **Windows XP Embedded:**
  1. Download Win XP Embedded file to USB stick
  2. Log in to printer console as administrator
  3. Insert USB Stick into machine
  4. Copy the Window XP update file to the Desktop
  5. Double Click the file to apply the update
  6. Restart machine

- **Windows 7 Embedded:**
  1. Download patch update zip file
  2. Unzip patch folder and download to USB stick
  3. Insert USB stick into machine
  4. Copy the patch folder to the desktop
  5. Open the folder
  6. Double click on the Win7 Embedded Patch x86.bat
  7. Restart machine

3D Production Printers
Customer Information Bulletin

Instructions and download links for each Printer line are included below:

SLS

ProX 500:

- Windows 7 Professional SP1 64-bit Operating System:
  1. Download patch **Win7 Standard Patch x64.zip** and copy to USB stick
  2. Insert USB stick into machine
  3. Copy **Win7 Standard Patch x64.zip** to the desktop and unzip it
  4. Open the folder
  5. Double click on the Win7 Standard Patch x64.bat to apply the update
  6. Restart machine as per update dialog
  7. Open “View update history” in “Windows Update”
  8. Verify Microsoft update KB4012212 is present and status is “Successful”

sPro 60 Printers running Sinter Software V5.0:

- Windows 7 Professional SP1 64-bit Operating System: Follow the same steps as listed for ProX 500.

3D Production Printers
Customer Information Bulletin

Instructions and download links for each Printer line are included below:

SLS

sPro 60/140/230 running latest Windows XP Image for PCs with new HD632-H81 motherboard and 225 MHz DSP:

NOTE: This update should also work for Windows XP Image running on old PCs with BL630 motherboard.

- **Windows XP SP3:**
  1. Download patch file win_XPSP3_embedded_windows and copy to USB stick
  2. Insert USB stick into machine
  3. Copy file to the desktop
  4. Double click on the **.exe** file to apply the update.
  5. Restart machine as per update dialog
  6. Open “Add or Remove Programs” in “Control Panel”
  7. Click “Show updates”
  8. Verify Microsoft update KB4012598 is present and status is “Installed”

Vanguard, Hi-Q and 2500 plus

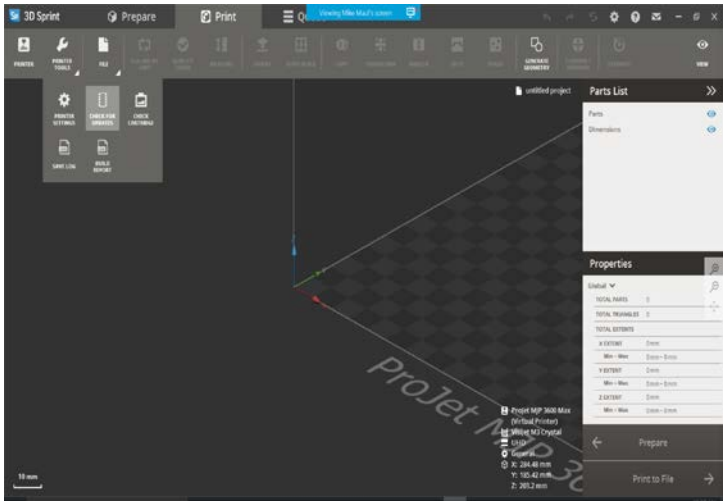
- Windows XP SP3 Operating System, follow the same steps as listed for sPro 60/140/230

3D Production Printers
Customer Information Bulletin

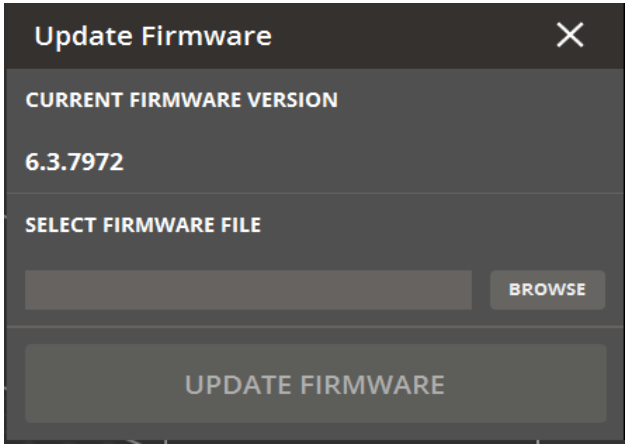
MJP

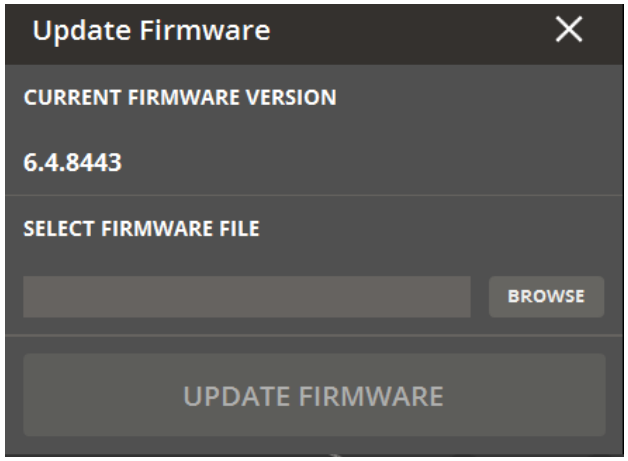
ProJet 3510/3600:

1. Download the appropriate UPD:
   a. 3510: ProJet 3510 Install.upd
   b. 3600: ProJet 3600 Install.upd
2. Run 3D Sprint 2.5
3. Under Print Set-Up tab, select Printer Tools
4. While holding CTRL-ALT-SHIFT left click Check for Updates

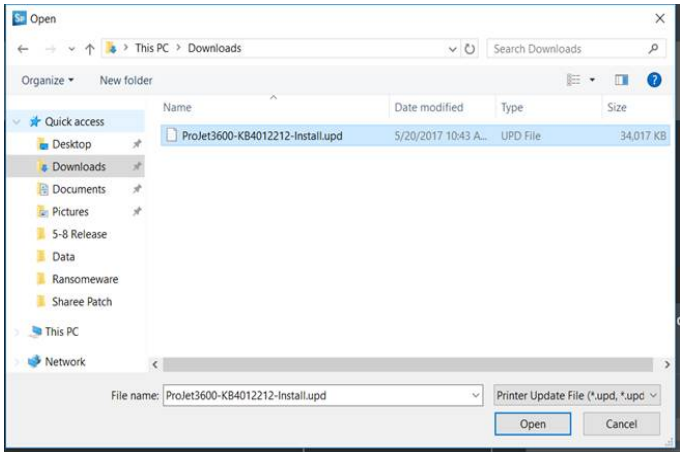


5. Click Browse to choose the UPD file

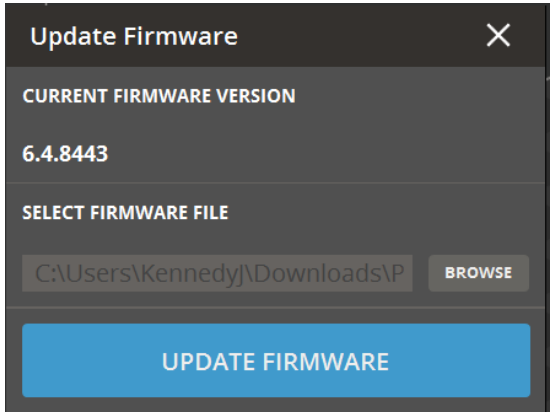


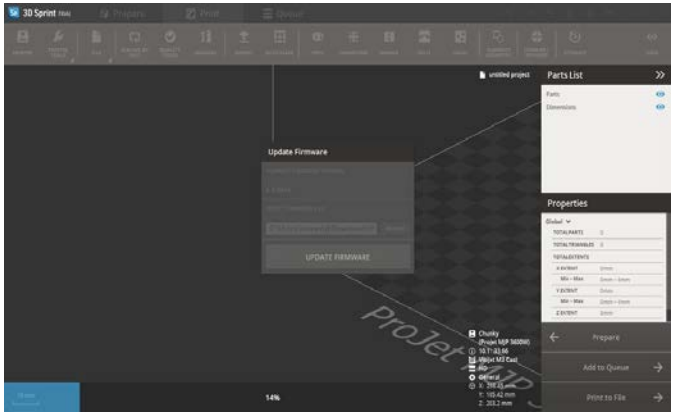


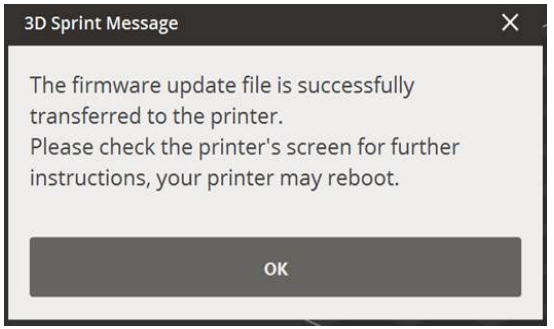
ProJet 3510/3600 Cont'd



6. Click "Update Firmware"







3D Production Printers
Customer Information Bulletin

ProJet 2500

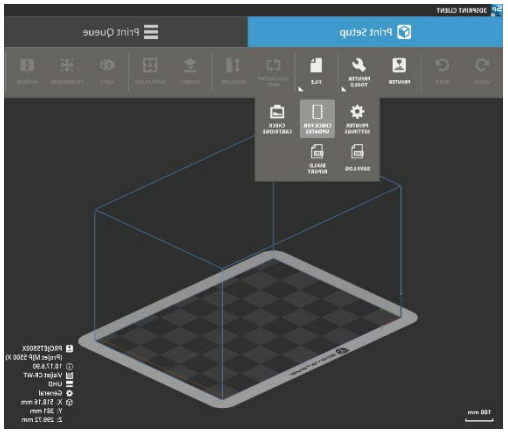
A new firmware .UPD file will be provided via 3D Sprint in the next few days. When you run 3D Sprint you will be offered to upgrade your printer firmware. Follow the steps to upgrade the firmware and the correct Microsoft patches will be applied to your system.

ProJet 5500X

Update your system using 3D Sprint:

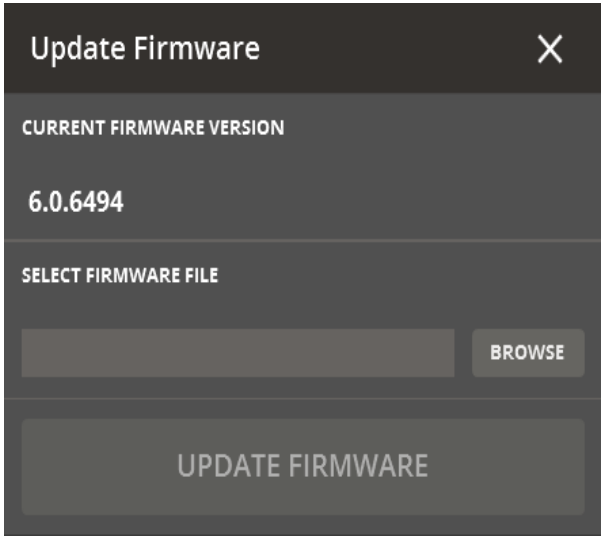
1. Download the UPD
2. Run 3D Sprint Client 1.1.136

3. Under Print Set-Up tab, select Printer Tools



ProJet 5500X Cont'd:

4. While holding CTRL-ALT-SHIFT left click Check for Updates
5. Left Click Browse button to select UPD file
6. Navigate to downloaded file ProJet5500-Install-RansomwarePatch-MS-KB4012212.upd
7. Left Click Update Firmware
8. Printer will auto-reboot



DMP

ProX 320, 100/200/300

Users or field service may always install all (critical) Windows Updates, it is not needed to install the 'optional' updates. From the Start Menu run Windows Updates manually (do not enable automatic Windows Updates) and apply all Critical updates. It is absolutely necessary to reboot Windows after the updates are installed.