

# Package Aware Print Driver MS16-087 - KB3170455



## Symptom

The new Microsoft Server Patch MS16-087 - KB3170455 requires print driver's to be packaged (Package Aware Printer Driver) in order for the client pc with non –administrator rights to install the print driver files.

# Affected products

All drivers are affected, even digitally signed WHQL drivers requires to be Package Aware Printer Driver.

### **Root Cause**

Recently a patch from Microsoft has been rolled out to their OS (Patch#: KB3170455). This patch is part of Microsoft's Security Update to resolve vulnerabilities in their Operating Systems. This security patch resolves Microsoft OS issue if an attacker is able to execute a man-in-the-middle (MiTM) attack on a workstation or a print server.

More details about this security patch from Microsoft, you can read it from this link: Microsoft Bulletin MS16-087.

### How does it affect us?

When the vulnerability of Microsoft has been addressed through installing the patch KB3170455, this requires the server to:

- Correct how the Windows Print Spooler writes to the file system
- Issuing a warning to users who attempt to install untrusted printer drivers
- Client PC connecting to the server requires Administrator rights to install the drivers

### Conclusion

WHQL drivers released from now on, will also be released as "Package Aware Printer Driver". However, there is no schedule (ETA) for the release dates of these drivers.

### Microsoft Package Aware Driver Workaround

As we cannot avoid this security settings, we advise our customer to do this workaround to make sure that the warning regarding untrusted printer drivers will not appear on client computers connecting to the server.

Procedure on <u>Client PC</u>:

- 1. Log on as Administrator on the Client PC.
- 2. Open Command Prompt, type "gpedit.msc" and then press [Enter]
- 3. You will have <u>Local Group Policy Editor</u> screen, go to User Configuration > Administrative Templates > Control Panel > Printers





4. Open "Point and Print Restrictions".





5. Select "Enabled" on "Point and Print Restrictions".



6. On the same group policy editor screen, look for Options; then check the [Users can only point and print to these servers] check box, and enter a server name into the [Enter fully qualified server names separated by semicolons] text box.

Point and Print Restrictions	and the state	
Point and Print Restriction:	5	Previous Setting Next Setting
<ul> <li>Not Configured Comme</li> <li>Enabled</li> </ul>	nt:	
Disabled		
Suppor	ted on: Supported	I Windows XP SP1 through Windows Server 2008 RTM
Options:		Help:
Users can only point and print	nt to these servers:	
Enter fully qualified server name semicolons	es separated by	This policy setting controls the client Point and Print behavior, including the security prompts for Windows Vista computers. The policy setting applies only to non-Print Administrator
Enter Server FQDN	Here	clients, and only to computers that are members of a domain.
Users can only point and print their forest	nt to machines in	When the policy setting is enabled: -Windows XP and later clients will only download print driver components from a list of explicitly named servers. If a

7. Select "Do not show warning or elevation prompt" for the option [When installing drivers for a new connection] selection box under Security Prompts:.

Options:		Help:
semicolons	*	
Enter Server FQDN here		This policy setting controls the client Point and Print behavior.
Users can only point and print to machines in their forest		including the security prompts for Windows Vista computers. The policy setting applies only to non-Print Administrator clients, and only to computers that are members of a domain.
Security Prompts:		When the policy setting is enabled: -Windows XP and later clients will only download print driver component from a list of endicities parent converse if a
When installing drivers for a new connection:		compatible print driver is available on the client, a printer
Do not show warning or elevation prompt 🔹 🔻	=	connection will be made. If a compatible print driver is not available on the client, no connection will be made.
when updating drivers for an existing connection:		-You can configure Windows Vista clients so that security warnings and elevated command prompts do not appear when users Point and Print, or when printer connection drivers need to be updated.
This setting only applies to:		
Windows Vista and later	-	-Windows Vista client computers can point and print to any
< III )		server.

8. Select "Do not show warning or elevation prompt" for the [When updating drivers for an existing connection] selection box under Security Prompts:.





- 9. Click [OK] and close the "Point and Print Restrictions" dialog box.
- 10. You are now back to Local Group Policy Editor screen, expand Computer Configuration > Administrative Templates > Printers

Local Group Policy Editor			
File Action View Help			
<ul> <li>Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Software Settings</li> <li>Administrative Templates</li> <li>Control Panel</li> <li>Control Panel</li> <li>Printers</li> <li>System</li> <li>System</li> <li>System</li> <li>System</li> <li>System</li> <li>Windows Components</li> <li>All Settings</li> <li>User Configuration</li> </ul>	Local Computer Policy Select an item to view its description.	Name	
	Extended Standard		



11. Open "Point and Print Restrictions".



12. Select "Enabled" on "Point and Print Restrictions".

Point and Print Res	strictions		×
Point and Print Re	estrictions	Previous Setting Next Setting	
<ul> <li>Not Configured</li> <li>Enabled</li> </ul>	Comment:		*
Disabled			Ŧ
	Supported on:	At least Windows Vista	*

- 13. On the same group policy editor screen, look for Options; then check the [Users can only point and print to these servers] check box, and enter a server name into the [Enter fully qualified server names separated by semicolons] text box.
- 14. Select "Do not show warning or elevation prompt" for the option [When installing drivers for a new connection] selection box under Security Prompts:.
- 15. Select "Do not show warning or elevation prompt" for the [When updating drivers for an existing connection] selection box under Security Prompts:.
- 16. Click [OK] and close the "Point and Print Restrictions" dialog box.
- 17. Close Local Group Policy Editor screen.





Point and Print Restrictions		
Point and Print Restrictions		Previous Setting Next Setting
<ul> <li>Not Configured Comment:</li> <li>Enabled</li> <li>Disabled</li> <li>Supported on:</li> </ul>		
Supported on:	At least Windows	Vista
Options:		Help:
<ul> <li>Users can only point and print to th Enter fully qualified server names separ semicolons</li> <li>Enter Server FQDN here</li> <li>Users can only point and print to me forest</li> <li>Security Prompts:</li> <li>When installing drivers for a new conn</li> <li>Do not show warning or elevation pro</li> <li>When updating drivers for an existing</li> <li>Do not show warning or elevation pro</li> <li>This setting only applies to:</li> </ul>	ese servers: ated by acchines in their ection: mpt v connection: mpt v	This policy setting controls the client Point and Print behavior, including the security prompts for Windows Vista computers. The policy setting applies only to non-Print Administrator clients, and only to computers that are members of a domain. When the policy setting is enabled: -Windows XP and later clients will only download print driver components from a list of explicitly named servers. If a compatible print driver is available on the client, a printer connection will be made. If a compatible print driver is not available on the client, no connection will be made. -You can configure Windows Vista clients so that security warnings and elevated command prompts do not appear when users Point and Print, or when printer connection drivers need to be updated. When the policy setting is not configured: -Windows Vista client computers will show a warning and an elevated command prompt when users create a printer connection to any server using Point and Print.

#### Notes:

For clients who participate in Active Directory, the above steps of changing Local Group Policy may not work since the Domain Group Policy could overwrite it.

In this case, you have to change the group policy applied to the client using the same procedure mentioned above. However, this should be done using the [Group Policy Management Console (GPMC)] tool on the server, so that the issue can be solved in the same manner without changing Local Group Policy on the client PC.

Since there are both "Computer Configuration" and "User Configuration" to setup on group policy editor, please make sure that you set up "Point and Print Restrictions" on both.

In order for you to check if a group policy setting has taken effect on the client pc, please use "*rsop.msc*" command on the pc.

