+

NCR ATM Security Update

DATE: July 16, 2021 **INCIDENT NO:** 2021-05 **REV:** #1

Print Spooler Vulnerability (AKA PrintNightMare)

Guidance and recommendations from NCR

Summary

Microsoft has published the details of a preliminary investigation on a vulnerability. Publicly Available Exploit code is available, and Windows out-of-band security patches are available for Windows 7 and Windows 10. View the Microsoft Advisory

What is the vulnerability?

The Microsoft Windows Print Spooler service fails to restrict access to functionality that allows users to add printers and related drivers, which can allow a remote authenticated attacker to execute arbitrary code with SYSTEM privileges on a vulnerable system.

ATMs that are connected to an Active Directory Domain are at risk. Any authenticated domain user could be used to change privileges to SYSTEM level and execute arbitrary code.

An ATM that is not connected to a domain is not at risk, unless the administrator password is shared and remote access has been enabled by relaxing group policies provided within Base OS Hardening (formerly Security for APTRA) that is provided with NCR consumer applications.

Guidance and Recommendation from NCR

For ATMs that are domain joined, the Microsoft July 2021 Out-of-band update is classified as critical and should be installed as soon as possible.

For ATMs that are not domain joined, NCR still recommends installing the Microsoft July 2021 Out-of-band update.

Please obtain the Microsoft July 2021 Out-of-band update from your usual channel. As with all Windows patches – the Windows "Servicing stack updates" are required in order to install the latest patches each month. For Windows 7 environments a customer would need to have licensed Windows 7 ESU to be able to access.

IMPORTANT NOTES for Windows 10 1809 environments only:

- Applying the Microsoft July 2021 Out-of-band update in a W10 1809 environment can introduce a problem where the correct USB touch screen calibration is lost. Installation of an updated touch screen component (i.e. USB Touch Screen Component 93.05.01.01 or later) will resolve this issue, so it is recommended that this is done immediately after installation of the Microsoft update. Contact your NCR Professional Services partner for assistance in getting this component. **Or apply the mitigation detailed below:**

- Applying the Microsoft July 2021 Out-of-band update in a W10 1809 environment will remove Adobe Flash. If you are still using Adobe Flash then **apply the mitigation detailed below**: -

Mitigation until it is possible to apply the Microsoft July 2021 Out-of-band update

For all Windows 7 and Windows 10 Environments, until it is possible to patch the ATM, the best option to ensure that customers' ATM estates are secure would be to disable inbound remote printing as per Microsoft's recommendation:

Configure the settings via Group Policy as follows:

1. Navigate to "Computer Configuration / Administrative Templates / Printers"
2. Set the "Allow Print Spooler to accept client connections:" value to "Disabled"
3. Restart the ATM, or restart the Print Spooler service

This policy will mitigate against remote attacks.

NOTE: You must restart the Print Spooler service, or ATM, for the group policy to take effect.

By Disabling inbound remote printing, remote machines will be unable to exploit the vulnerability. This, combined with the standard NCR Recommendations for protection against Logical Attacks (15 rules), will provide mitigation against this vulnerability until the patch can be applied.

Disable inbound remote printing:

- For machines where group policies are managed via Active Directory
  - Set the “Allow Print Spooler to accept client connections:” policy to the value “Disabled”

OR

- To apply the above group policy on machines where the group policies are not managed elsewhere then apply the following registry value:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers] "RegisterSpoolerRemoteRpcEndPoint" = dword:00000002
- THEN
  - Restart the Print Spooler service for the group policy to take effect.

    One of two methods of restarting the service can be used:

    - By rebooting the ATM
    - By running the following script:
      net stop spooler
      net start spooler

Additional details

- Full details of this patch release are available from Microsoft in their knowledgebase article.
- Full details of the vulnerability are available here.
- Contact your NCR account manager or NCR Professional Services Partner if you require help.
- In order to prevent malware (which could send commands locally to the print service) from becoming present on the ATM, the WNCR Logical Security – Requirements to Protect Against Logical Attacks Whitepaper details the full set of security controls that should be applied to protect ATMs against successful logical attacks.

Contacts

ATM Crime Reporting: global.security@ncr.com

Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com

Further information on this alert: owen.wild@ncr.com