NCR ATM SECURITY UPDATE

DATE: June 2019 **INCIDENT NO:** 2019-06 **REV:** #1

Microsoft Remote Desktop Services Vulnerability (aka Blue Keep)

Summary

On 14th May 2019 Microsoft released a patch designed to resolve a vulnerability in multiple Windows OS platforms. The vulnerability (also known as Blue Keep) was identified as CVE-2019-0708 and the summary issued by Microsoft is outlined below:

> *A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.*
> *To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.*
> *The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.*

Microsoft Guidance

Deploy 14th May 2019 Microsoft Security Update

Microsoft released security updates on May 14th, 2019 to mitigate against this vulnerability and the Microsoft recommendation is to install these updates as soon as possible. Guidance and these updates can be accessed via Microsoft Security Updates at the following:

NCR ATM SECURITY UPDATE

CVE-2019-0708 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708)

Customers and partners should pick up the Microsoft security update via their normal channel and test it prior to deployment to their live environment. Customers and partners who subscribe to NCR's Software Distribution Service should work with their NCR account team regarding deployment schedules.

NCR Guidance and Recommendations:

Customers should:

1. Turn off RDP and block the port on the external firewall to mitigate the vulnerability until the patch is applied
2. Test and then deploy the May 14th, 2019 patches made available by Microsoft as soon as possible.

As a reminder, by fully following the requirements within NCR Logical Security - Requirements to Protect Against Logical Attacks document and following common industry security practices customers are likely to be protected against any exploit of the vulnerability on their ATMs, specifically rule number 5 states:

> **RULE 5: REMOVE UNUSED SERVICES AND APPLICATIONS**
> It is recommended that you remove any unused services and applications from the system to reduce the attack surface area. By adopting the principle of 'If you don't use it, disable it', you remove potential points of attack by disabling modules and components that your application does not require.
> For example, if your application does not use output caching, you should disable the **ASP.NET** output cache module. Thereafter, if future security vulnerabilities are found in this module, your application is not vulnerable.

NCR ATM SECURITY UPDATE

The following table lists examples of the recommended applications that should be removed from the ATM software stack if they are not used on the ATM. However, you should review your software stack to determine if there are further binaries that can be removed:

Application	File Name	Description/Purpose
Address Resolution Protocol	arp.exe	Display/Edit network address
File Attribute	attrib.exe	Display/Edit file attributes
File Transfer Protocol	ftp.exe	Transfer files between two hosts
NetBios over TCP/IP	nbstat.exe	Display network information
Network Statistics	netstat.exe	Display network information
Name Server Lookup	nslookup.exe	Display network information
Remote Copy Package	rcp.exe	Copy files
Registry Editor	regedit.exe	Display/edit Windows registry
Registry Editor	regedt32.exe	Display/edit Windows registry
TCP/IP Route Command Application	route.exe	Display/edit network settings
Remote Shell Applications	rsh.exe	Execute command on remote computer
Terminal Emulation Protocol	telnet.exe	Connect to a remote computer

Contacts

ATM Crime Reporting: Global.Security@ncr.com

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

Please contact your NCR Account Manager if you have any questions or need additional information.