NEWSFLASH

Multiple Remote Code Execution Vulnerabilities in Microsoft Products

(CVE-2024-30080, CVE-2024-30103, CVE-2024-30078)

NANGIA & CO LLP

What are the different Vulnerabilities found in Microsoft Products?

Remote Code Execution via MSMQ:

An attacker can exploit the flaw in Microsoft Message Queuing component (MSMQ) by sending a specially crafted malicious MSMQ packet to a server with the MSMQ service enabled. Successful exploitation allows the attacker to execute arbitrary code on the server which may leads to takeover of the system. This vulnerability highlights the critical security concern for CVE-2024-30080.

Remote Code Execution via Outlook:

An attacker can exploit this vulnerability in Microsoft Outlook by bypassing the registry block lists to create and load malicious DLL files, which can execute without user interaction if the auto-open email feature is enabled. The vulnerability arises from improper handling of certain registry keys related to DLL handling and can be triggered by opening a specially crafted email in the Preview Pane. This vulnerability highlights the critical security concern for CVE-2024-30103.

Remote Code Execution using Wi-Fi Drivers:

The vulnerability in Windows Wi-Fi drivers arises from improper handling of SSIDs, leading to a buffer overflow when processing excessively long SSIDs without proper bounds checking. Attackers can exploit this by creating a malicious Wi-Fi access point with an excessively long SSID, allowing remote code execution when a device scans for networks, potentially compromising the entire system without user interaction. This vulnerability highlights the critical security concern for CVE-2024-30078.

What is affected?

Many Windows OS versions and Outlook versions are affected by this critical vulnerabilities which are, Affected Windows OS Versions with RCE using MSMQ(CVE-2024-30080) :

Windows 10: Versions 1809,21H2, 22H2, 1507, 1607

Windows 11 version 21H2, 22H2, 22H3, 23H2

Windows Server 2008 Service Pack 2, Windows Server 2008 Service Pack 2 (Server Core installation), Windows Server 2008 Service Pack 2, Windows Server 2008 R2 Service Pack 1, Windows Server 2008 R2 Service Pack 1 (Server Core installation)

Windows Server 2012, Windows Server 2012 (Server Core installation), Windows Server 2012 R2, Windows Server 2012 R2 (Server Core installation)

Windows Server 2016, Windows Server 2016 (Server Core installation)

Windows Server 2019, Windows Server 2019 (Server Core installation)

Windows Server 2022, Windows Server 2022, 23H2 (Server Core installation)

Affected Outlook Versions with RCE using outlook CVE-2024-30103 :

Microsoft Outlook 2013, Microsoft Outlook 2016, Microsoft Outlook 2019, Microsoft Outlook for Microsoft 365 (various builds).

Affected Windows OS version with RCE using Wi-Fi drivers CVE-2024-30078 :

Windows 10: Versions 21H2, 22H2; Windows 11: Versions 21H2, 22H2, 23H2; Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2

How to check if you are running a vulnerable version?

Here are a few steps to follow to check the running version of Outlook installed in system.

Step 1 Open Outlook

Step 2 Click on "File" in the top-left corner

Step 3 Select "Office Account“ or “Account” from the menu on the left

or

Step 3 Click on "Help" in the menu bar

Step 4 Click on "About Outlook" to see the version information

Here are a few steps to follow to check the running version of Operating System installed in system.

Step 1 Open Command prompt in windows system

Step 2 In the Command Prompt window, type ‘winver’ and press Enter. Detailed information about your Windows version will be displayed

What is the risk?

Remote Code Execution (RCE) vulnerabilities represent a critical security risk, enabling malicious actors to run arbitrary code on affected systems. This type of vulnerability can result in a complete takeover of the system, granting attackers the ability to access sensitive data without authorization and disrupt essential operations significantly. The potential for installing malicious software, elevating access privileges, and spreading infections across interconnected networks amplifies the threat, leading to extensive and possibly irreparable damage. The repercussions of such vulnerabilities are profound, encompassing data breaches, which compromise confidential information, and service interruptions that can halt business operations.

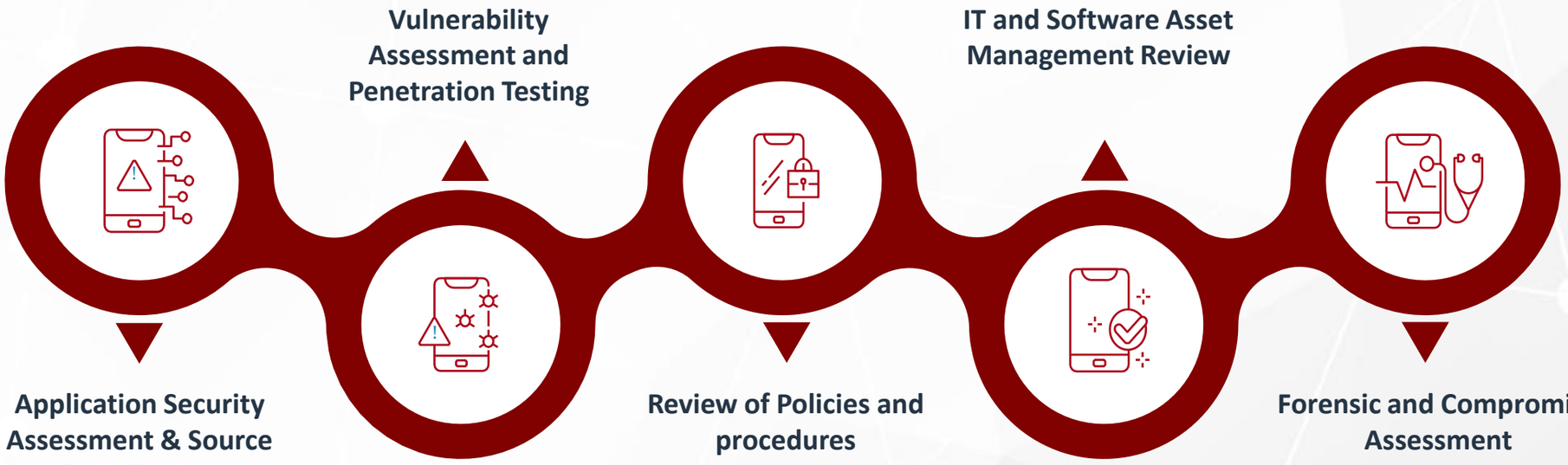
Denial-of-service vulnerability represents critical security risk, Attackers exploit this by overwhelming systems with a flood of requests that trigger numerous SHA-1 computations, consuming CPU resources excessively. This leads to degraded performance or complete unresponsiveness of the targeted systems, disrupting normal service availability. Upgrading to stronger hashing algorithms and optimizing cryptographic processes are crucial steps to mitigate such vulnerabilities effectively.

How Do You Protect Yourself?

Some of the steps that can be undertaken to protect the organization's infrastructure are:

1. It is suggested to disable MSMQ service, if the service is not required in your environment to prevent exploitation. If disabling MSMQ is not feasible, consider blocking inbound connections to TCP port 1801 from suspicious sources.
2. It is recommended to apply the security patches on Outlook provided by Microsoft. These patches address the underlying issue and prevent exploitation.
3. It is important to upgrade the Wi-Fi drivers with the latest security patches provided by Microsoft. Refrain from connecting to unknown or suspicious Wi-Fi networks. Also recommended to Employ security measures such as VPNs to protect data transmissions.
4. Conduct regular Vulnerability Assessment and Penetration tests for all public and internal facing information systems in your organization.
5. Conduct Comprise Assessments to proactively check for any signs of compromise of your IT environment.
6. Implement and enforce Patch Management Policy across the enterprise with special emphasis on critical systems

How Nangia & Co LLP can help?



NOIDA
(Delhi NCR - Corporate Office) A-109, Sector - 136, Noida - 201304, India
T: +91 120 2598000

GURUGRAM
001-005, Emaar Digital Greens Tower-A 10th Floor, Golf Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

CHENNAI
Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand Lights, Chennai - 600006 T: +91 44 46549201

PUNE
3rd Floor, Park Plaza, CTS 1085, Ganeshkhind Road, Next to Pune Central Mall, Shivajinagar, Pune - 411005, India

DELHI
(Registered Office) B-27, Soami Nagar, New Delhi - 110017, India T: +91 120 2598000

MUMBAI
4th Floor, Iconic Tower, URMI Estate, Ganpat Rao Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

BENGALURU
Prestige Obelisk, Level 4, No 3 Kasturba Road, Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

DEHRADUN
1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001, Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

Follow us at:

NANGIA & CO LLP