

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **Microsoft's April 2024 Patch Tuesday Addresses Two Zero-day Vulnerabilities**

Date of Publication

April 10, 2024

Admiralty Code

A1

TA Number

TA2024138
















# Summary

























**First Seen:** April 9, 2024

**Affected Platforms:** Microsoft Windows, Microsoft Azure Kubernetes, Microsoft Windows SmartScreen Prompt, Microsoft Windows Proxy Driver, Microsoft Defender for IoT, and Microsoft Windows DHCP Server

**Impact:** Denial of Service (DoS), Elevation of Privilege (EoP), Information Disclosure, Remote Code Execution (RCE), Spoofing, and Security Feature Bypass

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-26234	Microsoft Windows Proxy Driver Spoofing Vulnerability	Microsoft Windows Proxy Driver			
CVE-2024-29988	Microsoft Windows SmartScreen Prompt Security Feature Bypass Vulnerability	Microsoft Windows SmartScreen Prompt			
CVE-2024-29053	Microsoft Defender for IoT Remote Code Execution Vulnerability	Microsoft Defender for IoT			
CVE-2024-21323	Microsoft Defender for IoT Remote Code Execution Vulnerability	Microsoft Defender for IoT			
CVE-2024-21322	Microsoft Defender for IoT Remote Code Execution Vulnerability	Microsoft Defender for IoT			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-29990	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	Microsoft Azure Kubernetes			
CVE-2024-26158	Microsoft Install Service Elevation of Privilege Vulnerability	Microsoft Install Service			
CVE-2024-26209	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	Microsoft Local Security Authority Subsystem Service			
CVE-2024-26211	Microsoft Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-26212	Microsoft Windows DHCP Server Service Denial of Service Vulnerability	Microsoft Windows DHCP Server			
CVE-2024-26218	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-26230	Windows Telephony Server Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-26256	Microsoft Windows libarchive Remote Code Execution Vulnerability	Microsoft Windows			

# Vulnerability Details

## #1

Microsoft's April 2024 Patch Tuesday includes security updates for a total of 149 vulnerabilities, comprising three critical, 142 important, three moderate, and one low severity vulnerability. The breakdown of vulnerabilities includes 31 Elevation of Privilege, 27 Security Feature Bypass, 67 Remote Code Execution, 12 Information Disclosure, 7 Denial of Service, and 5 Spoofing vulnerabilities.

## #2

The updates cover various Microsoft products such as Office, SQL Server, .NET, Azure, Defender for IoT, Windows Kernel, Windows Hyper-V, Windows DHCP Server, Windows DNS Server, and more. Notably, Microsoft patched six non-Microsoft vulnerabilities, which include three Chromium-based Microsoft Edge browser vulnerabilities, bringing the total number of CVEs to 155. This advisory pertains to 13 CVEs that could potentially be exploited.

## #3

Two zero-day vulnerabilities have been fixed. The first one, CVE-2024-26234, is a proxy driver spoofing vulnerability linked to a malicious backdoor file within an Android screen mirroring app called LaiXi. Microsoft addressed this issue by revoking the relevant driver files.

## #4

The second exploited zero-day vulnerability, CVE-2024-29988, is a SmartScreen prompt security feature bypass associated with Water Hydra attacks. Security researchers confirm its exploitation, enabling bypassing of the Mark of the Web security feature. This flaw is similar to [CVE-2024-21412](#), previously exploited by Water Hydra to deliver DarkMe malware to financial traders, bypassing Microsoft Defender SmartScreen.

## #5

Microsoft Defender for IoT has been updated to address three critical remote code execution (RCE) vulnerabilities, however requiring local foothold on system. One vulnerability (CVE-2024-21322) requires administrative access, limiting its potential impact. These vulnerabilities could allow attackers to upload malicious files or overwrite existing files on Defender for IoT devices.

## #6

The Microsoft OLE DB Driver for SQL Server sees patches for 38 RCE vulnerabilities, possibly a record for a single component. Notably, there are no security patches for Exchange this month. Microsoft introduces Common Weakness Enumeration (CWE) assessments alongside CVSS data in advisories, providing deeper insights into vulnerabilities. The addition of CWE helps in understanding root causes, aiding developers in improving SDLC workflows and defenders in directing defense strategies effectively.

# Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-26234	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-284
CVE-2024-29988	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-693
CVE-2024-29053	Microsoft Defender for IoT: All versions	cpe:2.3:a:microsoft:defender_for_iot:*:*:*:*:*:*	CWE-36
CVE-2024-21323	Microsoft Defender for IoT: All versions	cpe:2.3:a:microsoft:defender_for_iot:*:*:*:*:*:*	CWE-36
CVE-2024-21322	Microsoft Defender for IoT: All versions	cpe:2.3:a:microsoft:defender_for_iot:*:*:*:*:*:*	CWE-77
CVE-2024-29990	Azure Kubernetes Service Confidential Containers: All versions	cpe:2.3:a:microsoft:azure_kubernetes_service_confidential_containers:*:*:*:*:*:*	CWE-284
CVE-2024-26158	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-59



CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-26209	Windows: 10 - 11 23H2 Windows Server: 2012 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-908
CVE-2024-26211	Windows: 10 - 11 23H2 Windows Server: 2012 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-122
CVE-2024-26212	Windows Server: 2008 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-400
CVE-2024-26218	Windows: 10 - 11 23H2 Windows Server: 2019 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-367
CVE-2024-26230	Windows: 10 - 11 23H2 Windows Server: 2008 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416
CVE-2024-26256	Windows: 11 22H2 - 11 23H2 Windows Server: 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-122

# Recommendations



Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential [patches](#) or adopting security measures.



Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.



Prioritize critical vulnerabilities, especially CVE-2024-26234 (Microsoft Windows Proxy Driver Spoofing Vulnerability) and CVE-2024-29988 (Microsoft Windows SmartScreen Prompt Security Feature Bypass Vulnerability). These vulnerabilities have the potential for severe exploitation and should be addressed urgently.



Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.



Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



## Potential MITRE ATT&CK TTPs

<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0042</u></b> Resource Development	<b><u>TA0007</u></b> Discovery	<b><u>TA0002</u></b> Execution
<b><u>TA0003</u></b> Persistence	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0040</u></b> Impact	<b><u>T1588.005</u></b> Exploits
<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1203</u></b> Exploitation for Client Execution

<b><u>T1082</u></b> System Information Discovery	<b><u>T1566</u></b> Phishing	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1498</u></b> Network Denial of Service
<b><u>T1036</u></b> Masquerading			

## Patch Details

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29990>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26158>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26209>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26211>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26212>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26218>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26230>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256>

## References

<https://msrc.microsoft.com/update-guide/releaseNote/2024-apr>

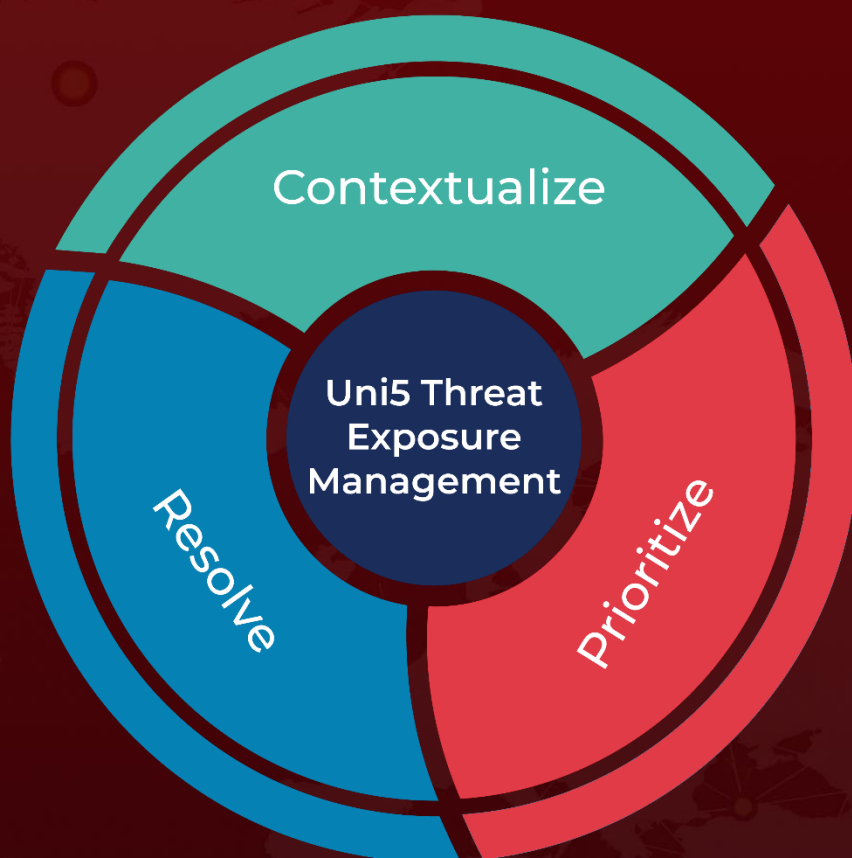
<https://www.hivepro.com/threat-advisory/water-hydra-exploits-cve-2024-21412-to-target-financial-traders/>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 10, 2024 • 11:30 PM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)