

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Microsoft's July 2023 Patch Tuesday Addresses 5 Zero-day Vulnerabilities

Date of Publication

July 12, 2023

Admiralty Code

A1

TA Number

TA2023296






















# Summary

**First Seen:** July 11, 2023

**Affected Platforms:** Windows, MS Office, Windows Defender SmartScreen, Windows MSHTML Platform, Outlook, Microsoft SharePoint Server

**Impact:** Remote Code Execution, Security Feature Bypass and Privilege Escalation

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-36874	Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability	Windows Error Reporting Service			
CVE-2023-32049	Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	Windows Defender SmartScreen			
CVE-2023-32046	Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability	Windows MSHTML Platform			
CVE-2023-36884	Office and Windows HTML Remote Code Execution Vulnerability	Office and Windows			
CVE-2023-35311	Microsoft Outlook Security Feature Bypass Vulnerability	Outlook			
CVE-2023-33160	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server			
CVE-2023-33157	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-35315	Microsoft Windows Remote Code Execution Vulnerability	Windows			
CVE-2023-32057	Microsoft Message Queuing Remote Code Execution Vulnerability	Windows			
CVE-2023-35297	Microsoft Windows Pragmatic General Multicast Remote Code Execution	Windows			
CVE-2023-35352	Microsoft Windows Remote Desktop unknown vulnerability	Windows			
CVE-2023-35367	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows			
CVE-2023-35366	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows			
CVE-2023-35365	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Windows			

# Vulnerability Details

## #1

Microsoft's July 2023 Patch Tuesday includes security updates for 130 flaws, including five actively exploited zero-day vulnerabilities, nine are rated as 'Critical', and 37 remote code execution vulnerabilities. One of the vulnerabilities remains unpatched and is actively exploited. Microsoft is investigating the issue however provided mitigation guidance for the same.

## #2

Notably, no Microsoft Edge vulnerabilities were addressed in this round of updates. The zero-day vulnerabilities include the elevation of privilege vulnerabilities, security feature bypass vulnerabilities, an HTML remote code execution vulnerability, and a Microsoft Outlook security feature bypass vulnerability.

## #3

Additionally, Microsoft has addressed the issue of malicious drivers abusing a Windows policy loophole to intercept browser traffic. They have revoked code-signing certificates and developer accounts associated with this activity.

## #4

Lastly, a zero-day vulnerability in Microsoft Outlook that allows bypassing security warnings in the preview pane has been fixed. The discloser of this vulnerability chose to remain anonymous.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36874	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-119
CVE-2023-32049	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-254
CVE-2023-32046	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-119

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36884	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Office: 2013 - 2019 Microsoft Word: 2013 Service Pack 1 - 2019	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-20
CVE-2023-35311	Microsoft Office: 2013 - 2019 Microsoft Outlook: 2013 - 2016 Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*	CWE-254
CVE-2023-33160	Microsoft SharePoint Server: 2019 - 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016 - 2016	cpe:2.3:a:microsoft:microsoft_sharepoint_server:2019:*:*:*:*:*	CWE-20
CVE-2023-33157	Microsoft SharePoint Server: 2019 - 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016 - 2016	cpe:2.3:a:microsoft:microsoft_sharepoint_server:2019:*:*:*:*:*	CWE-200
CVE-2023-35315	Windows: 10 - 11 22H2 Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-20
CVE-2023-32057	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-20
CVE-2023-35297	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*	CWE-20
CVE-2023-35352	Windows Server: 2012 - 2022 20H2	cpe:2.3:o:microsoft:windows_server:2019:*:*:*:*:*	CWE-254

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35367	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:win dows:10:1809:*:*:*:*:* :*	CWE-20
CVE-2023-35366			
CVE-2023-35365			

# Recommendations



**Apply Security Patches:** Immediately install the security patches released by Microsoft to address critical and high-severity vulnerabilities. Keep your software up to date by regularly checking for and applying the latest security updates and patches provided by the vendor. [CVE-2023-36884](#) lacks an official patch, but there are available [mitigation measures](#).



**Antivirus Software and Regular File Backup:** Use up-to-date antivirus software to detect and block any potential threats. Regularly back up your important files to a secure location, so you can recover them if your system is compromised. Use strong and unique passwords for all your accounts and enable two-factor authentication whenever possible.



**Remain vigilant:** Since the vulnerability was actively exploited, it's essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0004</u></b> Privilege Escalation
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588.005</u></b> Exploits
<b><u>T1203</u></b> Exploitation for Client Execution	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1068</u></b> Exploitation for Privilege Escalation	

## Patch Details

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33157>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35315>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35297>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35352>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35367>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35366>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35365>

## References

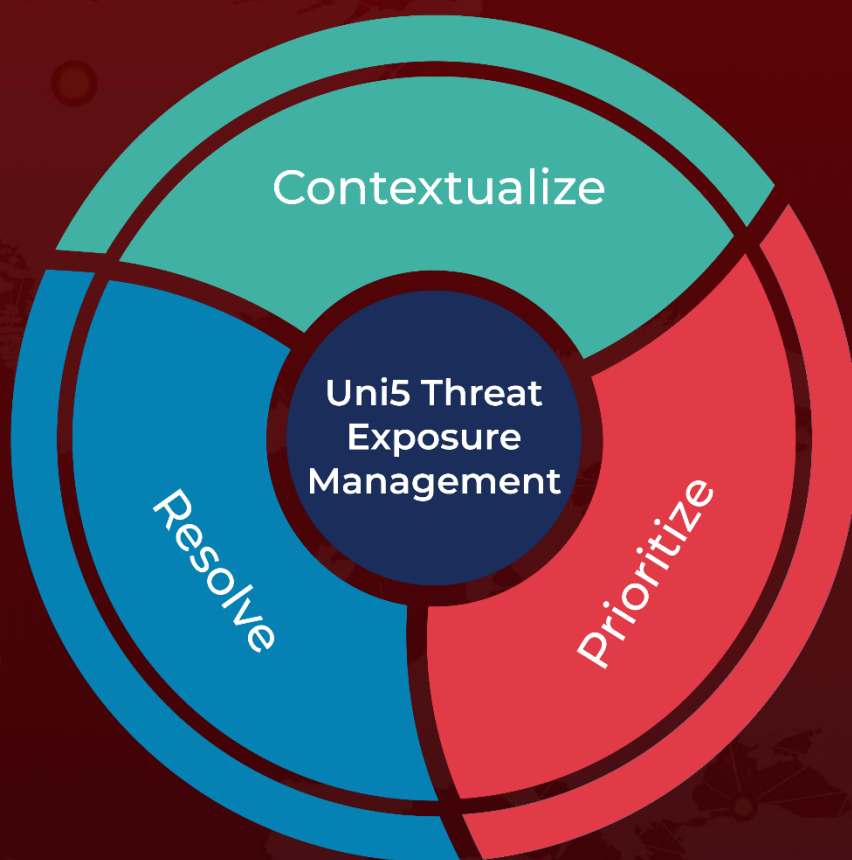
<https://www.tenable.com/blog/microsofts-july-2023-patch-tuesday-addresses-130-cves-cve-2023-36884>

<https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul>

# 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

**July 12, 2023 • 10:30 AM**

© 2023 All Rights are Reserved by HivePro



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