

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Microsoft's April 2026 Patch Tuesday

Date of Publication

April 16, 2026

Admiralty Code

A1

TA Number

TA2026102

# Summary

**First Seen:** April 14, 2026

**Affected Platforms:** Microsoft SQL Server, Windows Kernal, Windows Server Update Service, Microsoft Office, Microsoft SharePoint, Google Chromium and more

**Impact:** Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing, Tampering










## ⚙️ Exploitable CVEs

| CVE                           | NAME  | AFFECTED PRODUCT                         | ZERO-DAY | CISA KEV | PATCH |
|-------------------------------|---|--|----------|----------|-------|
| CVE-2026-32201                | Microsoft SharePoint Server Spoofing Vulnerability                            | Microsoft Office SharePoint              | ✓        | ✓        | ✓     |
| <a href="#">CVE-2026-5281</a> | Chromium Use after free in Dawn Vulnerability                                 | Microsoft Edge (Chromium-based)          | ✓        | ✓        | ✓     |
| CVE-2026-0390                 | UEFI Secure Boot Security Feature Bypass Vulnerability                        | Windows Boot Loader                      | ✗        | ✗        | ✓     |
| CVE-2026-26151                | Remote Desktop Spoofing Vulnerability   | Remote Desktop Spoofing                  | ✗        | ✗        | ✓     |
| CVE-2026-26169                | Windows Kernel Memory Information Disclosure Vulnerability                    | Windows Kernel                           | ✗        | ✗        | ✓     |
| CVE-2026-27906                | Windows Hello Security Feature Bypass Vulnerability                           | Windows Hello                            | ✗        | ✗        | ✓     |
| CVE-2026-27908                | Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability | Windows TDI Translation Driver (tdx.sys) | ✗        | ✗        | ✓     |
| CVE-2026-27909                | Windows Search Service Elevation of Privilege Vulnerability                   | Microsoft Windows Search Component       | ✗        | ✗        | ✓     |

**Note:** The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

| CVE            | NAME  | AFFECTED PRODUCT                                   | ZERO-DAY   | CISA KEV  | PATCH   |
|----------------|---|--|--|---|---|
| CVE-2026-27913 | Windows BitLocker Security Feature Bypass Vulnerability                             | Windows BitLocker                                  |    |    |    |
| CVE-2026-27914 | Microsoft Management Console Elevation of Privilege Vulnerability                   | Microsoft Management Console                       |    |    |    |
| CVE-2026-27921 | Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability       | Windows TDI Translation Driver                     |    |    |    |
| CVE-2026-32070 | Windows Common Log File System Driver Elevation of Privilege Vulnerability          | Windows Common Log File System Driver              |    |    |    |
| CVE-2026-32075 | Windows UPnP Device Host Elevation of Privilege Vulnerability                       | Windows Universal Plug and Play (UPnP) Device Host |    |    |    |
| CVE-2026-32093 | Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability | Function Discovery Service (fdwsd.dll)             |  |  |  |
| CVE-2026-32152 | Desktop Window Manager Elevation of Privilege Vulnerability                         | Desktop Window Manager                             |  |  |  |
| CVE-2026-32154 | Desktop Window Manager Elevation of Privilege Vulnerability                         | Desktop Window Manager                             |  |  |  |
| CVE-2026-32162 | Windows COM Elevation of Privilege Vulnerability                                    | Windows COM  |  |  |  |
| CVE-2026-32202 | Windows Shell Spoofing Vulnerability  | Windows Shell                                      |  |  |  |

**Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.**

| CVE            | NAME   | AFFECTED PRODUCT         | ZERO-DAY  | CISA KEV  | PATCH   |
|----------------|--|--------------------------|---|---|---|
| CVE-2026-32225 | Windows Shell Security Feature Bypass Vulnerability          | Windows Shell            |  |  |  |
| CVE-2026-33825 | Microsoft Defender Elevation of Privilege Vulnerability      | Microsoft Defender       |  |  |  |
| CVE-2026-33826 | Windows Active Directory Remote Code Execution Vulnerability | Windows Active Directory |  |  |  |

**Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.**

# Potential MITRE ATT&CK TTPs

| Tactic               | Technique  | Sub-technique                                       |
|----------------------|--|---|
| Initial Access       | <u>T1190</u> : Exploit Public-Facing Application     |   |
|                      | <u>T1189</u> : Drive-by Compromise                   |   |
|                      | <u>T1566</u> : Phishing                              | <u>T1566.001</u> : Spearphishing Attachment         |
|                      |  | <u>T1566.002</u> : Spearphishing Link               |
| Execution            | <u>T1203</u> : Exploitation for Client Execution     |   |
|                      | <u>T1059</u> : Command and Scripting Interpreter     | <u>T1059.001</u> : PowerShell                       |
|                      | <u>T1204</u> : User Execution                        | <u>T1204.001</u> : Malicious Link                   |
|                      |  | <u>T1204.002</u> : Malicious File                   |
| Defense Evasion      | <u>T1562</u> : Impair Defenses                       | <u>T1562.001</u> : Disable or Modify Tools          |
|                      | <u>T1553</u> : Subvert Trust Controls                | <u>T1553.005</u> : Mark-of-the-Web Bypass           |
|                      |  | <u>T1553.006</u> : Code Signing Policy Modification |
| Privilege Escalation | <u>T1068</u> : Exploitation for Privilege Escalation |   |
|                      | <u>T1542</u> : Pre-OS Boot                           | <u>T1542.003</u> : Bootkit                          |
| Credential Access    | <u>T1552</u> : Unsecured Credentials                 |   |
|                      | <u>T1556</u> : Modify Authentication Process         |   |
| Lateral Movement     | <u>T1021</u> : Remote Services                       | <u>T1021.001</u> : Remote Desktop Protocol          |
|                      | <u>T1210</u> : Exploitation of Remote Services       |   |
| Impact               | <u>T1499</u> : Endpoint Denial of Service            |   |

# Vulnerability Details

## #1

Microsoft's April 2026 Patch Tuesday delivers one of the most extensive security update releases in the company's history, addressing **165** vulnerabilities across its product ecosystem. Of these, 8 are rated Critical, 153 Important, 1 low and 3 Moderate. The vulnerabilities span multiple impact categories, including 93 Elevation of Privilege (EoP), 20 Remote Code Execution (RCE), 20 Information Disclosure, 12 Security Feature Bypass, 9 Denial of Service (DoS), 10 Spoofing, and 1 Tampering flaws. Elevation of Privilege vulnerabilities alone account for over 56% of this month's patches, reflecting the continued attacker focus on post-compromise privilege escalation as a critical link in modern attack chains.

## #2

Microsoft also resolved 82 non-Microsoft vulnerabilities, including Chromium-based Edge flaws, bringing the total number of CVEs addressed this month to **247**. This makes April 2026 one of the largest Patch Tuesday cycles on record, trailing only October 2025's 221 CVE release. Notably, 21 CVEs are assessed as either actively exploited or at increased risk of exploitation including 1 actively exploited in the wild, 1 publicly disclosed prior to patching, underscoring the urgency of rapid patch deployment.

## #3

The actively exploited CVE-2026-32201, is a Spoofing vulnerability in Microsoft SharePoint Server (CVSS 6.5) stemming from improper input validation. Despite its moderate CVSS score, confirmed wild exploitation, and SharePoint's role as a central collaboration platform make it the top remediation priority. The flaw likely manifests as cross-site scripting (XSS) and could allow attackers to view and modify sensitive organizational data. This follows a pattern of SharePoint zero-days being leveraged in ransomware and cyberespionage campaigns, similar to the ToolShell exploit chain observed in July 2025.

## #4

The publicly disclosed flaw, CVE-2026-33825, is an Elevation of Privilege vulnerability in Microsoft Defender (CVSS 7.8). While no active exploitation has been confirmed, the flaw's description closely matches "BlueHammer", a proof-of-concept exploit published on GitHub on April 3 by a researcher using the alias "Chaotic Eclipse". Systems with Microsoft Defender disabled are not in a vulnerable state.

## #5

Among the Chromium-based Edge vulnerabilities, CVE-2026-5281 zero-day (Use After Free in Dawn) stands out as it is confirmed exploited in the wild. Two additional Chromium flaws, CVE-2026-5858 and CVE-2026-5859, both in the WebML API, are rated Critical by Google with \$43,000 bounties each, and could allow remote code execution via crafted HTML pages.

## #6

The eight Critical vulnerabilities present serious network-level risk. CVE-2026-33824 (Windows IKE Service Extensions, CVSS 9.8) and CVE-2026-33827 (Windows TCP/IP, CVSS 8.1) are both unauthenticated, network-exploitable RCEs with wormable characteristics, the former targeting systems with IKE v2 enabled, the latter affecting IPv6/IPsec environments via a race condition. CVE-2026-33826 (Windows Active Directory, CVSS 8.0) enables authenticated RCE on domain controllers via crafted RPC calls.

## #7

Three Critical RCEs in Microsoft Word and Office (CVE-2026-33115, CVE-2026-33114, CVE-2026-32190) are exploitable through the Preview Pane without opening files, continuing a dangerous pattern from March 2026. CVE-2026-32157 (Remote Desktop Client, CVSS 8.8) targets users connecting to malicious RDP servers, and CVE-2026-23666 (.NET Framework) is a rare Critical-rated Denial of Service capable of crippling any network-facing .NET application.

## #8

Beyond these, the Secure Boot and BitLocker bypass flaws are particularly urgent given the Secure Boot certificate expiration deadline on June 26, 2026. This release also marks the end of Extended Security Updates for Exchange Server 2016 and 2019, leaving on-premises Exchange environments without security coverage. Organizations should prioritize patching internet-facing systems, domain controllers, SharePoint deployments, and endpoints with IKE/IPsec or IPv6 enabled, while validating Secure Boot certificate status across the fleet before the June deadline.

# Recommendations



Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible, particularly SharePoint Server, IKE/IPsec endpoints, and IPv6-enabled systems. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential patches or adopting interim security measures such as firewall rules for UDP ports 500 and 4500.



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 applications exposed to the internet, thoroughly review their configurations, including Secure Boot certificate status ahead of the June 26, 2026 expiration deadline.



Prioritize patching the actively exploited and critical vulnerabilities CVE-2026-32201, CVE-2026-5281, CVE-2026-33825, CVE-2026-33824, CVE-2026-33827, CVE-2026-33826, CVE-2026-33115, CVE-2026-33114, and CVE-2026-32190. These vulnerabilities pose significant exploitation risks, including wormable network RCEs and Preview Pane-based Office attacks, and should be addressed urgently.



Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This is especially critical given the wormable IKE and TCP/IP vulnerabilities and the Active Directory RCE that can enable lateral movement across domain-joined environments.



Adhere to the principle of "least privilege" by giving users only the essential permissions they need for their tasks. With Elevation of Privilege accounting for over 56% of this month's patches, this strategy is critical to reducing the impact of privilege escalation vulnerabilities.

# All CVEs

| CVE                                   | NAME  | PRODUCT   | IMPACT                  |
|---------------------------------------|---|---|-------------------------|
| <a href="#"><u>CVE-2026-0390</u></a>  | UEFI Secure Boot Security Feature Bypass Vulnerability                            | Windows Boot Loader                                 | Security Feature Bypass |
| <a href="#"><u>CVE-2026-20806</u></a> | Windows COM Server Information Disclosure Vulnerability                           | Windows COM   | Information Disclosure  |
| <a href="#"><u>CVE-2026-20928</u></a> | Windows Recovery Environment Security Feature Bypass Vulnerability                | Windows Recovery Environment Agent                  | Security Feature Bypass |
| <a href="#"><u>CVE-2026-20930</u></a> | Windows Management Services Elevation of Privilege Vulnerability                  | Windows Management Services                         | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-20945</u></a> | Microsoft SharePoint Server Spoofing Vulnerability                                | Microsoft Office SharePoint                         | Spoofing                |
| <a href="#"><u>CVE-2026-23653</u></a> | GitHub Copilot and Visual Studio Code Information Disclosure Vulnerability        | GitHub Copilot and Visual Studio Code               | Information Disclosure  |
| <a href="#"><u>CVE-2026-23657</u></a> | Microsoft Word Remote Code Execution Vulnerability                                | Microsoft Office Word                               | Remote Code Execution   |
| <a href="#"><u>CVE-2026-23666</u></a> | .NET Framework Denial of Service Vulnerability                                    | .NET Framework                                      | Denial of Service       |
| <a href="#"><u>CVE-2026-23670</u></a> | Windows Virtualization-Based Security (VBS) Security Feature Bypass Vulnerability | Windows Virtualization-Based Security (VBS) Enclave | Security Feature Bypass |

| <b>CVE</b>                   | <b>NAME</b>   | <b>PRODUCT</b>   | <b>IMPACT</b>           |
|------------------------------|---|--|-------------------------|
| <b><u>CVE-2026-25184</u></b> | Applocker Filter Driver (applockerfltr.sys) Elevation of Privilege Vulnerability          | Applocker Filter Driver (applockerfltr.sys)                | Elevation of Privilege  |
| <b><u>CVE-2026-26143</u></b> | Microsoft PowerShell Security Feature Bypass Vulnerability                                | Microsoft PowerShell                                       | Security Feature Bypass |
| <b><u>CVE-2026-26149</u></b> | Microsoft Power Apps Security Feature Bypass  | Microsoft Power Apps                                       | Security Feature Bypass |
| <b><u>CVE-2026-26151</u></b> | Remote Desktop Spoofing Vulnerability   | Windows Remote Desktop                                     | Spoofing                |
| <b><u>CVE-2026-26152</u></b> | Microsoft Cryptographic Services Elevation of Privilege Vulnerability                     | Windows Cryptographic Services                             | Elevation of Privilege  |
| <b><u>CVE-2026-26153</u></b> | Windows Encrypted File System (EFS) Elevation of Privilege Vulnerability                  | Windows Encrypting File System (EFS)                       | Elevation of Privilege  |
| <b><u>CVE-2026-26154</u></b> | Windows Server Update Service (WSUS) Tampering Vulnerability                              | Windows Server Update Service                              | Tampering               |
| <b><u>CVE-2026-26155</u></b> | Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability | Windows Local Security Authority Subsystem Service (LSASS) | Information Disclosure  |
| <b><u>CVE-2026-26156</u></b> | Windows Hyper-V Remote Code Execution Vulnerability                                       | Role: Windows Hyper-V                                      | Remote Code Execution   |
| <b><u>CVE-2026-26159</u></b> | Remote Desktop Licensing Service Elevation of Privilege Vulnerability                     | Windows Remote Desktop Licensing Service                   | Elevation of Privilege  |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>                                | <b>IMPACT</b>          |
|---------------------------------------|--|---|------------------------|
| <a href="#"><u>CVE-2026-26160</u></a> | Remote Desktop Licensing Service Elevation of Privilege Vulnerability              | Windows Remote Desktop Licensing Service      | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26161</u></a> | Windows Sensor Data Service Elevation of Privilege Vulnerability                   | Windows Sensor Data Service                   | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26162</u></a> | Windows OLE Elevation of Privilege Vulnerability                                   | Windows OLE                                   | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26163</u></a> | Windows Kernel Elevation of Privilege Vulnerability                                | Windows Kernel                                | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26165</u></a> | Windows Shell Elevation of Privilege Vulnerability                                 | Windows Shell                                 | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26166</u></a> | Windows Shell Elevation of Privilege Vulnerability                                 | Windows Shell                                 | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26167</u></a> | Windows Push Notifications Elevation of Privilege Vulnerability                    | Windows Push Notifications                    | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26168</u></a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock | Elevation of Privilege |
| <a href="#"><u>CVE-2026-26169</u></a> | Windows Kernel Memory Information Disclosure Vulnerability                         | Windows Kernel Memory                         | Information Disclosure |
| <a href="#"><u>CVE-2026-26170</u></a> | PowerShell Elevation of Privilege Vulnerability                                    | Microsoft PowerShell                          | Elevation of Privilege |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>                                | <b>IMPACT</b>           |
|---------------------------------------|--|---|-------------------------|
| <a href="#"><u>CVE-2026-26171</u></a> | .NET Denial of Service Vulnerability   | .NET  | Denial of Service       |
| <a href="#"><u>CVE-2026-26172</u></a> | Windows Push Notifications Elevation of Privilege Vulnerability                    | Windows Push Notifications                    | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26173</u></a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26174</u></a> | Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability          | Windows Server Update Service                 | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26175</u></a> | Windows Boot Manager Security Feature Bypass Vulnerability                         | Windows Boot Manager                          | Security Feature Bypass |
| <a href="#"><u>CVE-2026-26176</u></a> | Windows Client Side Caching driver (csc.sys) Elevation of Privilege Vulnerability  | Windows Client Side Caching driver (csc.sys)  | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26177</u></a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26178</u></a> | Windows Advanced Rasterization Platform Elevation of Privilege Vulnerability       | Windows Advanced Rasterization Platform       | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26179</u></a> | Windows Kernel Elevation of Privilege Vulnerability                                | Windows Kernel                                | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-26180</u></a> | Windows Kernel Elevation of Privilege Vulnerability                                | Windows Kernel                                | Elevation of Privilege  |

| <b>CVE</b>                                   | <b>NAME</b>  | <b>PRODUCT</b>                                | <b>IMPACT</b>           |
|--|--|---|-------------------------|
| <b><u><a href="#">CVE-2026-26181</a></u></b> | Microsoft Brokering File System Elevation of Privilege Vulnerability                   | Microsoft Brokering File System               | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-26182</a></u></b> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability     | Windows Ancillary Function Driver for WinSock | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-26183</a></u></b> | Remote Access Management service/API (RPC server) Elevation of Privilege Vulnerability | Windows RPC API                               | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-26184</a></u></b> | Windows Projected File System Elevation of Privilege Vulnerability                     | Windows Projected File System                 | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-27906</a></u></b> | Windows Hello Security Feature Bypass Vulnerability                                    | Windows Hello                                 | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-27907</a></u></b> | Windows Storage Spaces Controller Elevation of Privilege Vulnerability                 | Windows Storage Spaces Controller             | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-27908</a></u></b> | Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability          | Windows TDI Translation Driver (tdx.sys)      | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-27909</a></u></b> | Windows Search Service Elevation of Privilege Vulnerability                            | Microsoft Windows Search Component            | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-27910</a></u></b> | Windows Installer Elevation of Privilege Vulnerability                                 | Windows Installer                             | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-27911</a></u></b> | Windows User Interface Core Elevation of Privilege Vulnerability                       | Windows User Interface Core                   | Elevation of Privilege  |

| <b>CVE</b>                            | <b>NAME</b>   | <b>PRODUCT</b>   | <b>IMPACT</b>           |
|---------------------------------------|---|--|-------------------------|
| <a href="#"><u>CVE-2026-27912</u></a> | Windows Kerberos Elevation of Privilege Vulnerability   | Windows Kerberos   | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27913</u></a> | Windows BitLocker Security Feature Bypass Vulnerability                                       | Windows BitLocker  | Security Feature Bypass |
| <a href="#"><u>CVE-2026-27914</u></a> | Microsoft Management Console Elevation of Privilege Vulnerability                             | Microsoft Management Console                             | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27915</u></a> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                 | Windows Universal Plug and Play (UPnP) Device Host       | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27916</u></a> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                 | Windows Universal Plug and Play (UPnP) Device Host       | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27917</u></a> | Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) Elevation of Privilege Vulnerability | Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27918</u></a> | Windows Shell Elevation of Privilege Vulnerability  | Windows Shell  | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27919</u></a> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                 | Windows Universal Plug and Play (UPnP) Device Host       | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27920</u></a> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                 | Windows Universal Plug and Play (UPnP) Device Host       | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27921</u></a> | Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability                 | Windows TCP/IP   | Elevation of Privilege  |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>                                     | <b>IMPACT</b>           |
|---------------------------------------|--|--|-------------------------|
| <a href="#"><u>CVE-2026-27922</u></a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock      | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27923</u></a> | Desktop Window Manager Elevation of Privilege Vulnerability                        | Desktop Window Manager                             | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27924</u></a> | Desktop Window Manager Elevation of Privilege Vulnerability                        | Desktop Window Manager                             | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27925</u></a> | Windows UPnP Device Host Information Disclosure Vulnerability                      | Windows Universal Plug and Play (UPnP) Device Host | Information Disclosure  |
| <a href="#"><u>CVE-2026-27926</u></a> | Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability        | Windows Cloud Files Mini Filter Driver             | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27927</u></a> | Windows Projected File System Elevation of Privilege Vulnerability                 | Windows Projected File System                      | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27928</u></a> | Windows Hello Security Feature Bypass Vulnerability                                | Windows Hello                                      | Security Feature Bypass |
| <a href="#"><u>CVE-2026-27929</u></a> | Windows LUA File Virtualization Filter Driver Elevation of Privilege Vulnerability | Windows LUAFV                                      | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-27930</u></a> | Windows GDI Information Disclosure Vulnerability                                   | Windows GDI  | Information Disclosure  |
| <a href="#"><u>CVE-2026-27931</u></a> | Windows GDI Information Disclosure Vulnerability                                   | Windows GDI  | Information Disclosure  |

| <b>CVE</b>                                   | <b>NAME</b>  | <b>PRODUCT</b>   | <b>IMPACT</b>          |
|--|--|--|------------------------|
| <b><u><a href="#">CVE-2026-32068</a></u></b> | Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability | Windows SSDP Service                                       | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32069</a></u></b> | Windows Projected File System Elevation of Privilege Vulnerability                               | Windows Projected File System                              | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32070</a></u></b> | Windows Common Log File System Driver Elevation of Privilege Vulnerability                       | Windows Common Log File System Driver                      | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32071</a></u></b> | Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability       | Windows Local Security Authority Subsystem Service (LSASS) | Denial of Service      |
| <b><u><a href="#">CVE-2026-32072</a></u></b> | Active Directory Spoofing Vulnerability  | Windows Active Directory                                   | Spoofing               |
| <b><u><a href="#">CVE-2026-32073</a></u></b> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability               | Windows Ancillary Function Driver for WinSock              | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32074</a></u></b> | Windows Projected File System Elevation of Privilege Vulnerability                               | Windows Projected File System                              | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32075</a></u></b> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                    | Windows Universal Plug and Play (UPnP) Device Host         | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32076</a></u></b> | Windows Storage Spaces Controller Elevation of Privilege Vulnerability                           | Windows Storage Spaces Controller                          | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32077</a></u></b> | Windows UPnP Device Host Elevation of Privilege Vulnerability                                    | Windows Universal Plug and Play (UPnP) Device Host         | Elevation of Privilege |

| <b>CVE</b>                                   | <b>NAME</b>  | <b>PRODUCT</b>                         | <b>IMPACT</b>          |
|--|--|--|------------------------|
| <b><u><a href="#">CVE-2026-32078</a></u></b> | Windows Projected File System Elevation of Privilege Vulnerability                               | Windows Projected File System          | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32079</a></u></b> | Web Account Manager Information Disclosure Vulnerability   | Windows File Explorer                  | Information Disclosure |
| <b><u><a href="#">CVE-2026-32080</a></u></b> | Windows WalletService Elevation of Privilege Vulnerability                                       | Windows WalletService                  | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32081</a></u></b> | Package Catalog Information Disclosure Vulnerability   | Windows File Explorer                  | Information Disclosure |
| <b><u><a href="#">CVE-2026-32082</a></u></b> | Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability | Windows SSDP Service                   | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32083</a></u></b> | Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability | Windows SSDP Service                   | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32084</a></u></b> | Windows Print Spooler Information Disclosure Vulnerability                                       | Windows File Explorer                  | Information Disclosure |
| <b><u><a href="#">CVE-2026-32085</a></u></b> | Remote Procedure Call Information Disclosure Vulnerability                                       | Windows Remote Procedure Call          | Information Disclosure |
| <b><u><a href="#">CVE-2026-32086</a></u></b> | Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability              | Function Discovery Service (fdwsd.dll) | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32087</a></u></b> | Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability              | Function Discovery Service (fdwsd.dll) | Elevation of Privilege |

| <b>CVE</b>                            | <b>NAME</b>   | <b>PRODUCT</b>                         | <b>IMPACT</b>           |
|---------------------------------------|---|--|-------------------------|
| <a href="#"><u>CVE-2026-32088</u></a> | Windows Biometric Service Security Feature Bypass Vulnerability                     | Windows Biometric Service              | Security Feature Bypass |
| <a href="#"><u>CVE-2026-32089</u></a> | Windows Speech Brokered Api Elevation of Privilege Vulnerability                    | Windows Speech Brokered Api            | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32090</u></a> | Windows Speech Brokered Api Elevation of Privilege Vulnerability                    | Windows Speech Brokered Api            | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32091</u></a> | Microsoft Brokering File System Elevation of Privilege Vulnerability                | Microsoft Brokering File System        | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32093</u></a> | Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability | Function Discovery Service (fdwsd.dll) | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32149</u></a> | Windows Hyper-V Remote Code Execution Vulnerability                                 | Role: Windows Hyper-V                  | Remote Code Execution   |
| <a href="#"><u>CVE-2026-32150</u></a> | Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability | Function Discovery Service (fdwsd.dll) | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32151</u></a> | Windows Shell Information Disclosure Vulnerability                                  | Windows Shell                          | Information Disclosure  |
| <a href="#"><u>CVE-2026-32152</u></a> | Desktop Window Manager Elevation of Privilege Vulnerability                         | Desktop Window Manager                 | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32153</u></a> | Windows Speech Runtime Elevation of Privilege Vulnerability                         | Microsoft Windows Speech               | Elevation of Privilege  |

| <b>CVE</b>                                   | <b>NAME</b>  | <b>PRODUCT</b>   | <b>IMPACT</b>          |
|--|--|--|------------------------|
| <b><u><a href="#">CVE-2026-32154</a></u></b> | Desktop Window Manager<br>Elevation of Privilege<br>Vulnerability      | Desktop Window<br>Manager                                | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32155</a></u></b> | Desktop Window Manager<br>Elevation of Privilege<br>Vulnerability      | Desktop Window<br>Manager                                | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32156</a></u></b> | Windows UPnP Device Host<br>Remote Code Execution<br>Vulnerability     | Windows Universal<br>Plug and Play (UPnP)<br>Device Host | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-32157</a></u></b> | Remote Desktop Client<br>Remote Code Execution<br>Vulnerability        | Remote Desktop<br>Client                                 | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-32158</a></u></b> | Windows Push Notifications<br>Elevation of Privilege<br>Vulnerability  | Windows Push<br>Notifications                            | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32159</a></u></b> | Windows Push Notifications<br>Elevation of Privilege<br>Vulnerability  | Windows Push<br>Notifications                            | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32160</a></u></b> | Windows Push Notifications<br>Elevation of Privilege<br>Vulnerability  | Windows Push<br>Notifications                            | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32162</a></u></b> | Windows COM Elevation of<br>Privilege Vulnerability                    | Windows COM  | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32163</a></u></b> | Windows User Interface Core<br>Elevation of Privilege<br>Vulnerability | Windows User<br>Interface Core                           | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-32164</a></u></b> | Windows User Interface Core<br>Elevation of Privilege<br>Vulnerability | Windows User<br>Interface Core                           | Elevation of Privilege |

| CVE                                   | NAME   | PRODUCT                                       | IMPACT                 |
|---------------------------------------|--|---|------------------------|
| <a href="#"><u>CVE-2026-32165</u></a> | Windows User Interface Core Elevation of Privilege Vulnerability                   | Windows User Interface Core                   | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32167</u></a> | SQL Server Elevation of Privilege Vulnerability                                    | SQL Server                                    | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32168</u></a> | Azure Monitor Agent Elevation of Privilege Vulnerability                           | Azure Monitor Agent                           | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32171</u></a> | Azure Logic Apps Elevation of Privilege Vulnerability                              | Azure Logic Apps                              | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32176</u></a> | SQL Server Elevation of Privilege Vulnerability                                    | SQL Server                                    | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32178</u></a> | .NET Spoofing Vulnerability  | .NET  | Spoofing               |
| <a href="#"><u>CVE-2026-32181</u></a> | Connected User Experiences and Telemetry Service Denial of Service Vulnerability   | Microsoft Windows                             | Denial of Service      |
| <a href="#"><u>CVE-2026-32183</u></a> | Windows Snipping Tool Remote Code Execution Vulnerability                          | Windows Snipping Tool                         | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32184</u></a> | Microsoft High Performance Compute (HPC) Pack Elevation of Privilege Vulnerability | Microsoft High Performance Compute Pack (HPC) | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32188</u></a> | Microsoft Excel Information Disclosure Vulnerability                               | Microsoft Office Excel                        | Information Disclosure |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>              | <b>IMPACT</b>          |
|---------------------------------------|--|-----------------------------|------------------------|
| <a href="#"><u>CVE-2026-32189</u></a> | Microsoft Excel Remote Code Execution Vulnerability      | Microsoft Office Excel      | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32190</u></a> | Microsoft Office Remote Code Execution Vulnerability     | Microsoft Office            | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32192</u></a> | Azure Monitor Agent Elevation of Privilege Vulnerability | Azure Monitor Agent         | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32195</u></a> | Windows Kernel Elevation of Privilege Vulnerability      | Windows Kernel              | Elevation of Privilege |
| <a href="#"><u>CVE-2026-32196</u></a> | Windows Admin Center Spoofing Vulnerability              | Windows Admin Center        | Spoofing               |
| <a href="#"><u>CVE-2026-32197</u></a> | Microsoft Excel Remote Code Execution Vulnerability      | Microsoft Office Excel      | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32198</u></a> | Microsoft Excel Remote Code Execution Vulnerability      | Microsoft Office Excel      | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32199</u></a> | Microsoft Excel Remote Code Execution Vulnerability      | Microsoft Office Excel      | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32200</u></a> | Microsoft PowerPoint Remote Code Execution Vulnerability | Microsoft Office PowerPoint | Remote Code Execution  |
| <a href="#"><u>CVE-2026-32201</u></a> | Microsoft SharePoint Server Spoofing Vulnerability       | Microsoft Office SharePoint | Spoofing               |

| <b>CVE</b>                                   | <b>NAME</b>   | <b>PRODUCT</b>                                      | <b>IMPACT</b>           |
|--|---|---|-------------------------|
| <b><u><a href="#">CVE-2026-32202</a></u></b> | Windows Shell Spoofing Vulnerability                                      | Windows Shell                                       | Spoofing                |
| <b><u><a href="#">CVE-2026-32203</a></u></b> | .NET and Visual Studio Denial of Service Vulnerability                    | .NET and Visual Studio                              | Denial of Service       |
| <b><u><a href="#">CVE-2026-32212</a></u></b> | Universal Plug and Play (upnp.dll) Information Disclosure Vulnerability   | Universal Plug and Play (upnp.dll)                  | Information Disclosure  |
| <b><u><a href="#">CVE-2026-32214</a></u></b> | Universal Plug and Play (upnp.dll) Information Disclosure Vulnerability   | Universal Plug and Play (upnp.dll)                  | Information Disclosure  |
| <b><u><a href="#">CVE-2026-32215</a></u></b> | Windows Kernel Information Disclosure Vulnerability                       | Windows Kernel                                      | Information Disclosure  |
| <b><u><a href="#">CVE-2026-32216</a></u></b> | Windows Redirected Drive Buffering System Denial of Service Vulnerability | Windows Redirected Drive Buffering                  | Denial of Service       |
| <b><u><a href="#">CVE-2026-32217</a></u></b> | Windows Kernel Information Disclosure Vulnerability                       | Windows Kernel                                      | Information Disclosure  |
| <b><u><a href="#">CVE-2026-32218</a></u></b> | Windows Kernel Information Disclosure Vulnerability                       | Windows Kernel                                      | Information Disclosure  |
| <b><u><a href="#">CVE-2026-32219</a></u></b> | Microsoft Brokering File System Elevation of Privilege Vulnerability      | Microsoft Brokering File System                     | Elevation of Privilege  |
| <b><u><a href="#">CVE-2026-32220</a></u></b> | UEFI Secure Boot Security Feature Bypass Vulnerability                    | Windows Virtualization-Based Security (VBS) Enclave | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-32221</a></u></b> | Windows Graphics Component Remote Code Execution Vulnerability            | Microsoft Graphics Component                        | Remote Code Execution   |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>                                | <b>IMPACT</b>           |
|---------------------------------------|--|---|-------------------------|
| <a href="#"><u>CVE-2026-32222</u></a> | Windows Win32k Elevation of Privilege Vulnerability                                | Windows Win32K - ICOMP                        | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32223</u></a> | Windows USB Printing Stack (usbprint.sys) Elevation of Privilege Vulnerability     | Windows USB Print Driver                      | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32224</u></a> | Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability          | Windows Server Update Service                 | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-32225</u></a> | Windows Shell Security Feature Bypass Vulnerability                                | Windows Shell                                 | Security Feature Bypass |
| <a href="#"><u>CVE-2026-32226</u></a> | .NET Framework Denial of Service Vulnerability                                     | .NET Framework                                | Denial of Service       |
| <a href="#"><u>CVE-2026-33095</u></a> | Microsoft Word Remote Code Execution Vulnerability                                 | Microsoft Office Word                         | Remote Code Execution   |
| <a href="#"><u>CVE-2026-33096</u></a> | HTTP.sys Denial of Service Vulnerability   | Windows HTTP.sys                              | Denial of Service       |
| <a href="#"><u>CVE-2026-33098</u></a> | Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability  | Windows Container Isolation FS Filter Driver  | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-33099</u></a> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock | Elevation of Privilege  |

| <b>CVE</b>                                   | <b>NAME</b>  | <b>PRODUCT</b>                                | <b>IMPACT</b>          |
|--|--|---|------------------------|
| <b><u><a href="#">CVE-2026-33100</a></u></b> | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Windows Ancillary Function Driver for WinSock | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-33101</a></u></b> | Windows Print Spooler Elevation of Privilege Vulnerability                         | Windows Print Spooler Components              | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-33103</a></u></b> | Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability          | Microsoft Dynamics 365 (on-premises)          | Information Disclosure |
| <b><u><a href="#">CVE-2026-33104</a></u></b> | Win32k Elevation of Privilege Vulnerability  | Windows Win32K - GRFX                         | Elevation of Privilege |
| <b><u><a href="#">CVE-2026-33114</a></u></b> | Microsoft Word Remote Code Execution Vulnerability                                 | Microsoft Office Word                         | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-33115</a></u></b> | Microsoft Word Remote Code Execution Vulnerability                                 | Microsoft Office Word                         | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-33116</a></u></b> | .NET, .NET Framework, and Visual Studio Denial of Service Vulnerability            | .NET, .NET Framework, Visual Studio           | Denial of Service      |
| <b><u><a href="#">CVE-2026-33118</a></u></b> | Microsoft Edge (Chromium-based) Spoofing Vulnerability                             | Microsoft Edge (Chromium-based)               | Spoofing               |
| <b><u><a href="#">CVE-2026-33119</a></u></b> | Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability                 | Microsoft Edge (Chromium-based)               | Spoofing               |
| <b><u><a href="#">CVE-2026-33120</a></u></b> | Microsoft SQL Server Remote Code Execution Vulnerability                           | SQL Server                                    | Remote Code Execution  |

| <b>CVE</b>                            | <b>NAME</b>  | <b>PRODUCT</b>                              | <b>IMPACT</b>           |
|---------------------------------------|--|---|-------------------------|
| <a href="#"><u>CVE-2026-33822</u></a> | Microsoft Word Information Disclosure Vulnerability  | Microsoft Office Word                       | Information Disclosure  |
| <a href="#"><u>CVE-2026-33824</u></a> | Windows Internet Key Exchange (IKE) Service Extensions Remote Code Execution Vulnerability | Windows IKE Extension                       | Remote Code Execution   |
| <a href="#"><u>CVE-2026-33825</u></a> | Microsoft Defender Elevation of Privilege Vulnerability                                    | Microsoft Defender                          | Elevation of Privilege  |
| <a href="#"><u>CVE-2026-33826</u></a> | Windows Active Directory Remote Code Execution Vulnerability                               | Windows Active Directory                    | Remote Code Execution   |
| <a href="#"><u>CVE-2026-33827</u></a> | Windows TCP/IP Remote Code Execution Vulnerability   | Windows TCP/IP                              | Remote Code Execution   |
| <a href="#"><u>CVE-2026-33829</u></a> | Windows Snipping Tool Spoofing Vulnerability   | Windows Snipping Tool                       | Spoofing                |
| <a href="#"><u>CVE-2023-20585</u></a> | AMD IOMMU Write Buffer Vulnerability   | Input-Output Memory Management Unit (IOMMU) | Tampering               |
| <a href="#"><u>CVE-2026-21637</u></a> | HackerOne TLS PSK/ALPN Callback Exceptions Bypass Error Handlers Vulnerability             | Node.js                                     | Denial of Service       |
| <a href="#"><u>CVE-2026-25250</u></a> | MITRE Secure Boot disable Eazy Fix Vulnerability   | Windows Secure Boot                         | Security Feature Bypass |
| <a href="#"><u>CVE-2026-32631</u></a> | GitHub 'git clone' from manipulated repositories can leak NTLM hashes Vulnerability        | GitHub Repo: Git for Windows                | Information Disclosure  |

| <b>CVE</b>                           | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>           |
|--------------------------------------|--|---------------------------------|-------------------------|
| <a href="#"><u>CVE-2026-5272</u></a> | Chromium Heap buffer overflow in GPU Vulnerability               | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5273</u></a> | Chromium Use after free in CSS Vulnerability                     | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5274</u></a> | Chromium Integer overflow in Codecs Vulnerability                | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5275</u></a> | Chromium Heap buffer overflow in ANGLE Vulnerability             | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5276</u></a> | Chromium Insufficient policy enforcement in WebUSB Vulnerability | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <a href="#"><u>CVE-2026-5277</u></a> | Chromium Integer overflow in ANGLE Vulnerability                 | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5279</u></a> | Chromium Object corruption in V8 Vulnerability                   | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5280</u></a> | Chromium Use after free in WebCodecs Vulnerability               | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5281</u></a> | Chromium Use after free in Dawn Vulnerability                    | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5283</u></a> | Chromium Inappropriate implementation in ANGLE Vulnerability     | Microsoft Edge (Chromium-based) | Remote Code Execution   |

| <b>CVE</b>                                  | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>          |
|---|--|---------------------------------|------------------------|
| <b><u><a href="#">CVE-2026-5284</a></u></b> | Chromium Use after free in Dawn Vulnerability                | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5285</a></u></b> | Chromium Use after free in WebGL Vulnerability               | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5286</a></u></b> | Chromium Use after free in Dawn Vulnerability                | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5287</a></u></b> | Chromium Use after free in PDF Vulnerability                 | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5289</a></u></b> | Chromium Use after free in Navigation Vulnerability          | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5290</a></u></b> | Chromium Use after free in Compositing Vulnerability         | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5291</a></u></b> | Chromium Inappropriate implementation in WebGL Vulnerability | Microsoft Edge (Chromium-based) | Information Disclosure |
| <b><u><a href="#">CVE-2026-5292</a></u></b> | Chromium Out of bounds read in WebCodecs Vulnerability       | Microsoft Edge (Chromium-based) | Information Disclosure |
| <b><u><a href="#">CVE-2026-5858</a></u></b> | Chromium Heap buffer overflow in WebML Vulnerability         | Microsoft Edge (Chromium-based) | Remote Code Execution  |
| <b><u><a href="#">CVE-2026-5859</a></u></b> | Chromium Integer overflow in WebML Vulnerability             | Microsoft Edge (Chromium-based) | Remote Code Execution  |

| <b>CVE</b>                           | <b>NAME</b>   | <b>PRODUCT</b>                  | <b>IMPACT</b>         |
|--------------------------------------|---|---------------------------------|-----------------------|
| <a href="#"><u>CVE-2026-5860</u></a> | Chromium Use after free in WebRTC Vulnerability           | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5861</u></a> | Chromium Use after free in V8 Vulnerability               | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5862</u></a> | Chromium Inappropriate implementation in V8 Vulnerability | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5863</u></a> | Chromium Inappropriate implementation in V8 Vulnerability | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5864</u></a> | Chromium Heap buffer overflow in WebAudio Vulnerability   | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5865</u></a> | Chromium Type Confusion in V8 Vulnerability               | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5866</u></a> | Chromium Use after free in Media Vulnerability            | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5867</u></a> | Chromium Heap buffer overflow in WebML Vulnerability      | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5868</u></a> | Chromium Heap buffer overflow in ANGLE Vulnerability      | Microsoft Edge (Chromium-based) | Remote Code Execution |
| <a href="#"><u>CVE-2026-5869</u></a> | Chromium Heap buffer overflow in WebML Vulnerability      | Microsoft Edge (Chromium-based) | Remote Code Execution |

| <b>CVE</b>                           | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>           |
|--------------------------------------|--|---------------------------------|-------------------------|
| <a href="#"><u>CVE-2026-5870</u></a> | Chromium Integer overflow in Skia Vulnerability                            | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5871</u></a> | Chromium Type Confusion in V8 Vulnerability                                | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5872</u></a> | Chromium Use after free in Blink Vulnerability                             | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5873</u></a> | Chromium Out of bounds read and write in V8 Vulnerability                  | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5874</u></a> | Chromium Use after free in PrivateAI Vulnerability                         | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5875</u></a> | Chromium Policy bypass in Blink Vulnerability                              | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <a href="#"><u>CVE-2026-5876</u></a> | Chromium Side-channel information leakage in Navigation Vulnerability      | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <a href="#"><u>CVE-2026-5877</u></a> | Chromium Use after free in Navigation Vulnerability                        | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <a href="#"><u>CVE-2026-5878</u></a> | Chromium Incorrect security UI in Blink Vulnerability                      | Microsoft Edge (Chromium-based) | Spoofing                |
| <a href="#"><u>CVE-2026-5879</u></a> | Chromium Insufficient validation of untrusted input in ANGLE Vulnerability | Microsoft Edge (Chromium-based) | Denial of Service       |

| <b>CVE</b>                                  | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>           |
|---|--|---------------------------------|-------------------------|
| <b><u><a href="#">CVE-2026-5880</a></u></b> | Chromium Incorrect security UI in browser UI Vulnerability                     | Microsoft Edge (Chromium-based) | Spoofting               |
| <b><u><a href="#">CVE-2026-5881</a></u></b> | Chromium Policy bypass in LocalNetworkAccess Vulnerability                     | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5882</a></u></b> | Chromium Incorrect security UI in Fullscreen Vulnerability                     | Microsoft Edge (Chromium-based) | Spoofting               |
| <b><u><a href="#">CVE-2026-5883</a></u></b> | Chromium Use after free in Media Vulnerability                                 | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <b><u><a href="#">CVE-2026-5884</a></u></b> | Chromium Insufficient validation of untrusted input in Media Vulnerability     | Microsoft Edge (Chromium-based) | Denial of Service       |
| <b><u><a href="#">CVE-2026-5885</a></u></b> | Chromium Insufficient validation of untrusted input in WebML Vulnerability     | Microsoft Edge (Chromium-based) | Denial of Service       |
| <b><u><a href="#">CVE-2026-5886</a></u></b> | Chromium Out of bounds read in WebAudio Vulnerability                          | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <b><u><a href="#">CVE-2026-5887</a></u></b> | Chromium Insufficient validation of untrusted input in Downloads Vulnerability | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5888</a></u></b> | Chromium Uninitialized Use in WebCodecs Vulnerability                          | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <b><u><a href="#">CVE-2026-5889</a></u></b> | Chromium Cryptographic Flaw in PDFium Vulnerability                            | Microsoft Edge (Chromium-based) | Security Feature Bypass |

| <b>CVE</b>                                  | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>           |
|---|--|---------------------------------|-------------------------|
| <b><u><a href="#">CVE-2026-5890</a></u></b> | Chromium Race in WebCodecs Vulnerability                             | Microsoft Edge (Chromium-based) | Denial of Service       |
| <b><u><a href="#">CVE-2026-5891</a></u></b> | Chromium Insufficient policy enforcement in browser UI Vulnerability | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5892</a></u></b> | Chromium Insufficient policy enforcement in PWAs Vulnerability       | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5893</a></u></b> | Chromium Race in V8 Vulnerability                                    | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <b><u><a href="#">CVE-2026-5894</a></u></b> | Chromium Inappropriate implementation in PDF Vulnerability           | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <b><u><a href="#">CVE-2026-5895</a></u></b> | Chromium Incorrect security UI in Omnibox Vulnerability              | Microsoft Edge (Chromium-based) | Spoofing                |
| <b><u><a href="#">CVE-2026-5896</a></u></b> | Chromium Policy bypass in Audio Vulnerability                        | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5897</a></u></b> | Chromium Incorrect security UI in Downloads Vulnerability            | Microsoft Edge (Chromium-based) | Spoofing                |
| <b><u><a href="#">CVE-2026-5898</a></u></b> | Chromium Incorrect security UI in Omnibox Vulnerability              | Microsoft Edge (Chromium-based) | Spoofing                |
| <b><u><a href="#">CVE-2026-5899</a></u></b> | Chromium Incorrect security UI in History Navigation Vulnerability   | Microsoft Edge (Chromium-based) | Spoofing                |

| <b>CVE</b>                                  | <b>NAME</b>  | <b>PRODUCT</b>                  | <b>IMPACT</b>           |
|---|--|---------------------------------|-------------------------|
| <b><u><a href="#">CVE-2026-5900</a></u></b> | Chromium Policy bypass in Downloads Vulnerability            | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5901</a></u></b> | Chromium Policy bypass in DevTools Vulnerability             | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5902</a></u></b> | Chromium Race in Media Vulnerability                         | Microsoft Edge (Chromium-based) | Denial of Service       |
| <b><u><a href="#">CVE-2026-5903</a></u></b> | Chromium Policy bypass in IFrameSandbox Vulnerability        | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <b><u><a href="#">CVE-2026-5904</a></u></b> | Chromium Use after free in V8 Vulnerability                  | Microsoft Edge (Chromium-based) | Remote Code Execution   |
| <b><u><a href="#">CVE-2026-5905</a></u></b> | Chromium Incorrect security UI in Permissions Vulnerability  | Microsoft Edge (Chromium-based) | Spoofing                |
| <b><u><a href="#">CVE-2026-5906</a></u></b> | Chromium Incorrect security UI in Omnibox Vulnerability      | Microsoft Edge (Chromium-based) | Spoofing                |
| <b><u><a href="#">CVE-2026-5907</a></u></b> | Chromium Insufficient data validation in Media Vulnerability | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <b><u><a href="#">CVE-2026-5908</a></u></b> | Chromium Integer overflow in Media Vulnerability             | Microsoft Edge (Chromium-based) | Denial of Service       |
| <b><u><a href="#">CVE-2026-5909</a></u></b> | Chromium Integer overflow in Media Vulnerability             | Microsoft Edge (Chromium-based) | Denial of Service       |

| CVE                                  | NAME  | PRODUCT                         | IMPACT                  |
|--------------------------------------|---|---------------------------------|-------------------------|
| <a href="#"><u>CVE-2026-5910</u></a> | Chromium Integer overflow in Media Vulnerability                                | Microsoft Edge (Chromium-based) | Denial of Service       |
| <a href="#"><u>CVE-2026-5911</u></a> | Chromium Policy bypass in ServiceWorkers Vulnerability                          | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <a href="#"><u>CVE-2026-5912</u></a> | Chromium Integer overflow in WebRTC Vulnerability                               | Microsoft Edge (Chromium-based) | Denial of Service       |
| <a href="#"><u>CVE-2026-5913</u></a> | Chromium Out of bounds read in Blink Vulnerability                              | Microsoft Edge (Chromium-based) | Information Disclosure  |
| <a href="#"><u>CVE-2026-5914</u></a> | Chromium Type Confusion in CSS Vulnerability                                    | Microsoft Edge (Chromium-based) | Denial of Service       |
| <a href="#"><u>CVE-2026-5915</u></a> | Chromium Insufficient validation of untrusted input in WebML Vulnerability      | Microsoft Edge (Chromium-based) | Denial of Service       |
| <a href="#"><u>CVE-2026-5918</u></a> | Chromium Inappropriate implementation in Navigation Vulnerability               | Microsoft Edge (Chromium-based) | Security Feature Bypass |
| <a href="#"><u>CVE-2026-5919</u></a> | Chromium Insufficient validation of untrusted input in WebSockets Vulnerability | Microsoft Edge (Chromium-based) | Security Feature Bypass |

## References

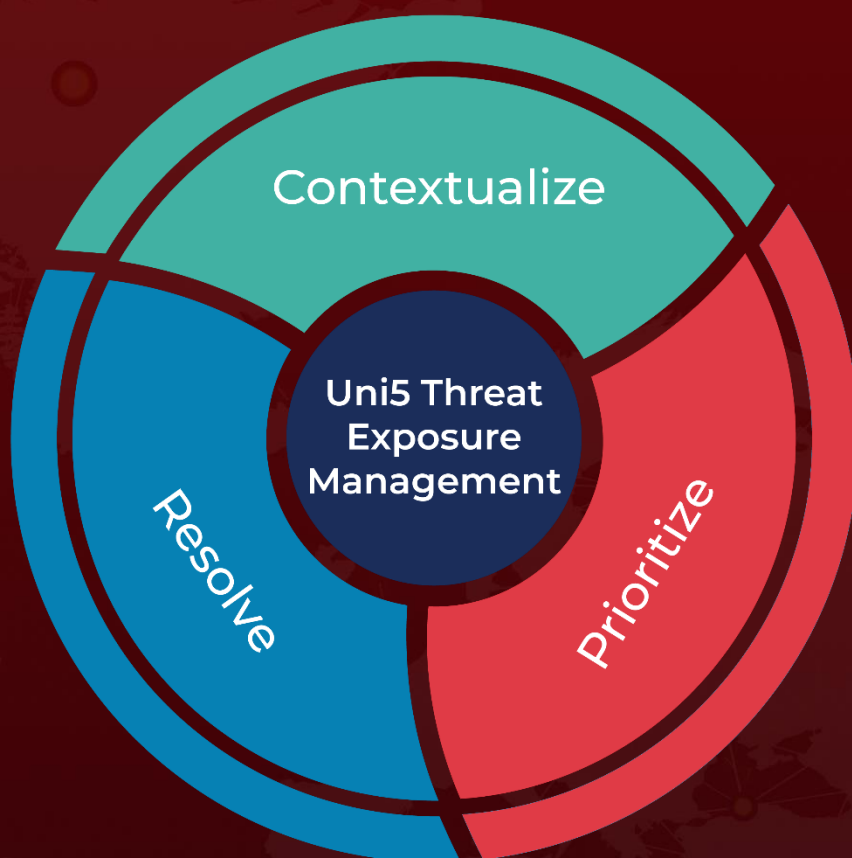
<https://msrc.microsoft.com/update-guide/releaseNote/2026-apr>

<https://hivepro.com/threat-advisory/cve-2026-5281-chrome-dawn-flaw-sparks-in-the-wild-zero-day-attacks/>

# 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 16, 2026 • 7:30 AM**

© 2026 All Rights are Reserved by Hive Pro



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