TLP:CLEAR

RadioCSIRT — Microsoft Patch Tuesday April 2026

Technical Analysis · April 14, 2026 · 167 CVEs · 8 Critical · 2 Zero-Days

EXPLOITED ZERO-DAY — CVE-2026-32201
Microsoft SharePoint Server Spoofing · CVSS 6.5 · Active exploitation confirmed. Affected: SharePoint 2016, 2019, Subscription Edition.

PUBLICLY DISCLOSED + PoC — CVE-2026-33825 (BlueHammer)
Microsoft Defender EoP · CVSS 7.8 · Exploit code published on GitHub April 3, 2026 by "Chaotic Eclipse". Auto-patch via Defender Platform 4.18.26050.3011.

01 Executive Summary & Context

167	8	2	20	93	21	13	10	9
Total CVEs	Critical	Zero-Days	RCE	EoP	Info Disc.	SFB	DoS	Spoofing

Microsoft's April 2026 Patch Tuesday is one of the largest releases of the year with 167 CVEs patched (excluding 80 Edge/Chromium vulnerabilities handled by Google). It ranks as the second-largest monthly release, behind only October 2025. Of the 167 vulnerabilities, 8 are rated Critical (7 RCE, 1 DoS) and 2 are Zero-Days.

The distribution reveals Elevation of Privilege (EoP) dominating at 57.1%, reflecting an exceptionally broad post-exploitation surface. An attacker with limited initial access has an unusually wide selection of vectors to reach SYSTEM or Domain Administrator privileges.

CVE Breakdown by Product Family — MSRC Source

Product Family	Sev.	RCE	EoP	Info	SFB	DoS	SPF	CVSS Max
Windows 11 v26H1	Crit	8	78	16	8	4	4	9.8
Windows 11 v25H2/v24H2	Crit	8	80	16	8	3	4	9.8
Windows 11 v23H2	Crit	7	77	16	7	3	4	9.8
Windows Server 2025	Crit	9	81	16	8	3	4	9.8
Windows Server 2022	Crit	8	80	16	9	3	4	9.8
Windows Server 2019	Crit	8	68	14	9	1	4	9.8
Windows Server 2016	Crit	8	52	12	8	1	4	9.8
Remote Desktop Client	Crit	1	—	—	—	—	—	8.8
Microsoft Office	Crit	10	—	2	—	—	—	8.4
Microsoft SharePoint	Imp	—	—	—	—	—	2	6.5
Microsoft .NET	Crit	—	—	—	—	5	1	7.5
SQL Server	Imp	1	2	—	—	—	—	8.8

Microsoft Azure	Imp	—	4	—	—	—	—	8.8
Microsoft Dynamics	Imp	—	—	1	1	—	—	9.0
PowerShell	Imp	—	—	—	1	—	—	7.8

Notable highlights this cycle

- First AMD CVE in a Microsoft Patch Tuesday: CVE-2023-20585 (AMD IOMMU Write Buffer) — integrated 3 years after the CVE ID was assigned.
- Node.js included for the first time: CVE-2026-21637 (TLS PSK/ALPN callback bypass — Moderate).
- New RDP anti-phishing protection for .rdp files (CVE-2026-26151, credited to NCSC UK — Exploitation More Likely).
- Progressive rollout of new Secure Boot certificates replacing 2011 certificates expiring in June 2026.
- Fix for a Microsoft Account sign-in regression introduced in March 2026 (Teams, Microsoft services).

02 Zero-Day Vulnerabilities — Technical Analysis

CVE-2026-32201 ZERO-DAY EXPLOITÉ Important

Microsoft SharePoint Server Spoofing Vulnerability CVSS 6.5

Component SharePoint 2016, 2019, Subscription Edition	**Type** Spoofing / Improper Input Validation
Vector AV:N / AC:L / PR:N / UI:N	**Impact** Confidentiality + Integrity (no Availability impact)
Status ⚠ **Active exploitation confirmed**	**Reporter** Not disclosed by Microsoft

Improper input validation in SharePoint allows an unauthenticated network attacker to perform spoofing operations. Real-world impact is limited per the MSRC vector: C:Low/I:Low/A:None. However, the "Exploitation detected" status warrants emergency treatment. SharePoint Online (Microsoft 365) is managed by Microsoft — no customer action required.

```
Components  : SharePoint 2016, 2019, Subscription Edition
Exploitability : Exploitation detected (MSRC)
SharePoint Online : managed by Microsoft, no customer action required
```

Action : Immediately patch all exposed on-premises SharePoint instances. Enable SharePoint access audit logs.

CVE-2026-33825 ZERO-DAY PoC PUBLIC Important

Microsoft Defender Elevation of Privilege — BlueHammer CVSS 7.8

Component Microsoft Defender Antimalware Platform	**Type** Elevation of Privilege → SYSTEM
Vector AV:L / AC:L / PR:L / UI:N (local, compte standard)	**Public exploit** BlueHammer — GitHub — Apr 3, 2026 by "Chaotic Eclipse"
Fix Defender Platform 4.18.26050.3011 (auto-deployed)	**Exploitabilité** **Exploitation More Likely (MSRC)**

EoP in Microsoft Defender allowing any local standard user to reach SYSTEM. BlueHammer exploit code was public for 11 days before the patch — the researcher raised concerns about Microsoft's disclosure process. The fix is delivered via the Defender platform independently of the standard Windows Update channel.

```
Verify  : Get-MpComputerStatus | Select-Object AMProductVersion
Target version : >= 4.18.26050.3011
Via            : Windows Security → Virus & threat protection → Protection updates
```

Action : Verify fleet-wide deployment (WSUS/MDM may lag). PoC public for 11 days — high exploitation risk on unpatched systems.

03 Critical Vulnerabilities — MSRC Analysis

CVE-2026-33824 Critique Exploitation Less Likely
Windows IKE Service Extensions — Remote Code Execution CVSS 9.8

Attack Vector **Network — NON AUTHENTIFIÉ (PR:None, UI:None)**	**Complexity** Low (AC:L)
Condition IKEv2 enabled on target	**Exposed ports** UDP/500 (IKE) · UDP/4500 (NAT-T)
Scope All supported Windows versions	**MSRC Exploitability** Exploitation Less Likely (malgré CVSS 9.8)

The most severe vulnerability this cycle at CVSS 9.8. Crafted IKEv2 packets → unauthenticated RCE. Important note: despite the maximum CVSS, MSRC rates this "Exploitation Less Likely" — indicating real-world implementation complexity not captured by the CVSS score. VPN/IPsec environments, DirectAccess, and any Windows system with IKEv2 enabled are at risk.

```
Full vector : AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Surface     : Any Windows system with IKEv2 enabled
```

Action : Temporary mitigation: block inbound UDP/500 and UDP/4500 via firewall rules until the patch is applied.

CVE-2026-33826 Critique Exploitation More Likely
Windows Active Directory — Remote Code Execution via RPC CVSS 8.0

Attack Vector **ADJACENT (AV:A) — same network segment as target DC**	**Authentication** Authenticated account required (PR:Low)
Scope Windows Server 2016, 2019, 2022, 2025 (not client workstations)	**MSRC Exploitability** **Exploitation More Likely**

RCE via crafted RPC call to a vulnerable RPC host. MSRC vector is Adjacent (AV:A) — the attacker must be on the same network segment as the target Domain Controller, not merely in the same AD domain. Classic lateral movement vector post-Initial Access. Server scope only: workstations are not affected.

Action : Prioritize patching on Domain Controllers. Monitor abnormal RPC calls from unexpected network segments.

CVE-2026-33827 Critique Exploitation Less Likely
Windows TCP/IP — Remote Code Execution CVSS 8.1

Attack Vector Network — AV:N / AC:HIGH / PR:None / UI:None	**Complexity** HIGH (AC:H) — specific technical condition not disclosed
Scope All supported Windows versions	**MSRC Exploitability** Exploitation Less Likely

RCE in the Windows TCP/IP stack. The CVSS 8.1 score reflects AC:High — unlike EternalBlue (AC:Low), this vulnerability requires a specific technical condition. MSRC rates it "Exploitation Less Likely". Maximum exposure surface (all Windows versions on the network) but large-scale exploitation is less probable in the near term.

CVE-2026-33115 · CVE-2026-33114 · CVE-2026-32190 Critique
Microsoft Office / Word — RCE via volet de prévisualisation CVSS 8.4

Components	Attack Vector
Word (LTSC 2021/2024, M365), Office générique, Excel, PowerPoint	Local — AV:L / AC:L / PR:None / UI:None (MSRC)
Phishing vector	**Scope**
Preview Pane — no document open required	M365 Apps, Office LTSC 2021/2024, Office 2019

Multiple Critical RCEs in the Office suite. CVE-2026-33115 and CVE-2026-33114 (Word) are triggerable via the Preview Pane without opening the document. The MSRC AV:L vector indicates local exploitation (file read), consistent with an email attachment phishing vector. Combine with CVE-2026-32200 (PowerPoint RCE) and Excel CVEs (32199, 32198, 32197, 32189).

```
CVE-2026-32190 : Office RCE — Critique — CVSS 8.4
CVE-2026-33115 : Word RCE — Critique — Preview Pane
CVE-2026-33114 : Word RCE — Critique — Preview Pane
CVE-2026-32200 : PowerPoint RCE — Important
CVE-2026-32199/98/97/89 : Excel RCE — Important (x4)
```

Action : Prioritize Office patching across all workstations. Consider disabling the Preview Pane for Office files until the patch is deployed.

CVE-2026-32157 Critique Exploitation Less Likely
Remote Desktop Client — Remote Code Execution CVSS 8.8

Attack Vector	Target
Network — AV:N / AC:L / PR:None / UI:Required	Client workstations (mstsc.exe) — not servers only
Scope	
All supported Windows versions	

RCE in the Remote Desktop client. A malicious or compromised RDP server can execute code on the connecting client workstation. User interaction required (UI:R) means the user must initiate the RDP connection. Particularly relevant in remote work environments and for targeting administrators.

CVE-2026-27913 Important Exploitation More Likely
Windows BitLocker — Secure Boot Security Feature Bypass CVSS 7.7

Type	MSRC Exploitability
Security Feature Bypass — Secure Boot / BitLocker TPM bypass	**Exploitation More Likely**
Context	
Physical access likely required	

Bypasses Secure Boot, breaking the BitLocker/TPM trust chain. Allows execution of unsigned software at startup. Priority for mobile fleets, remote work devices, and any hardware with unmonitored physical access risk.

04 Notable CVEs — MSRC-Confirmed Vectors

The following CVEs were highlighted by Microsoft in the official MSRC bulletin of April 14, 2026, due to their technical complexity, scope, or impact potential.

CVE-2026-26167 Important Exploitation Less Likely
Windows Push Notifications — Elevation of Privilege CVSS 8.8

Attack Vector	Scope
Local — AV:L / AC:L / PR:Low / UI:None	**CHANGED (S:C) — escalation crosses component boundary**
Scope	
All supported Windows versions	

EoP in the Push Notifications service with CVSS Scope:Changed on a local vector — the escalation crosses the component boundary, potentially impacting out-of-sandbox resources. CVSS 8.8 despite a local vector. A prime post-exploitation chaining candidate.

CVE-2026-32225 Important Exploitation More Likely
Windows Shell — Security Feature Bypass CVSS 8.8

Attack Vector	MSRC Exploitability
Network — AV:N / AC:L / PR:None / UI:Required	**Exploitation More Likely**
Scope	
All supported Windows versions	

Windows Shell SFB rated "Exploitation More Likely" with a network vector requiring no authentication. User interaction required (UI:R) points to a malicious document or social engineering delivery. Chainable with an EoP for a full exploitation sequence.

CVE-2026-27928 Important Exploitation Less Likely
Windows Hello — Security Feature Bypass CVSS 8.7

Attack Vector	Scope
Network — AV:N / AC:High / PR:None / UI:None	**CHANGED (S:C) — cross-component impact**
Scope	
Windows Server 2016 to 2025	

Windows Hello SFB with Scope:Changed and a network vector with no prerequisites. High complexity (AC:H) limits mass exploitation, but the no-authentication network vector with Scope:Changed makes it a target for advanced actors against server-side Windows authentication infrastructure.

CVE-2026-32162 Important Exploitation More Likely
Windows COM — Elevation of Privilege CVSS 8.4

Attack Vector	MSRC Exploitability
Local — AV:L / AC:L / PR:None / UI:None	**Exploitation More Likely**
Scope	
Windows 11 + Windows Server 2019, 2022, 2025	

EoP in the Windows COM component with no privileges or interaction required. "Exploitation More Likely". COM is ubiquitous in Windows and a prime post-Initial Access escalation vector from any standard user account.

CVE-2026-27912 Important Exploitation Less Likely
Windows Kerberos — Elevation of Privilege CVSS 8.0

Attack Vector	Authentication
ADJACENT — AV:A / même segment réseau que le serveur cible	PR:Low — compte authentifié requis
Scope	
Windows Server 2016, 2019, 2022, 2025 (not client workstations)	

EoP in Kerberos with an Adjacent vector (AV:A) — the attacker must be on the same network segment as the target server. Server-only scope (2016 to 2025). Relevant for an attacker already positioned on the internal network seeking to escalate privileges against Kerberos authentication infrastructure.

CVE-2026-26151 Important Exploitation More Likely

Remote Desktop Spoofing — Protection anti-phishing .rdp (NCSC UK) CVSS 7.1

Discovered by	Vector
UK National Cyber Security Centre (NCSC)	Fichier .rdp malveillant ouvert par l'utilisateur
MSRC Exploitability	
Exploitation More Likely — exploitation réelle probable	

Before this fix, opening an .rdp file triggered no security warning. Post-patch, Remote Desktop displays all requested connection settings, disabled by default, with a one-time warning on first use. NCSC UK attribution suggests real-world exploitation in live campaigns. .rdp files are a documented phishing vector to bypass MFA on RDP connections.

```
New behavior post-patch:
- ALL connection settings displayed before connecting
- All settings disabled by default
- One-time warning on first use per device
```

05 Prioritization Matrix — CISO / SOC / VOC

Priority	CVE	Component	Timeline	Rationale
P0	CVE-2026-32201	SharePoint	**Immediate (0h)**	Zero-day exploited in the wild. All on-premises SharePoint instances.
P0	CVE-2026-33825	Defender	**Immediate (auto)**	PoC public 11 days. Verify 4.18.26050.3011 fleet-wide.
P1	CVE-2026-33824	Windows IKE	**24–48h**	CVSS 9.8, network, unauthenticated. Mitigate UDP/500+4500 immediately.
P1	CVE-2026-33115/14	Office Word	**24–48h**	Critical RCE via Preview Pane. Active phishing vector.
P1	CVE-2026-33826	Active Directory	**48–72h**	AD RCE (AV:Adjacent). Exploitation More Likely. Patch Domain Controllers first.
P1	CVE-2026-33827	TCP/IP Stack	**48–72h**	Critical RCE network stack (AC:H — less trivial than EternalBlue).
P2	CVE-2026-32157	RDP Client	72h–1 week	Critical RCE RDP client. Prioritize admin workstations.
P2	CVE-2026-32225	Windows Shell	1 week	Network SFB, Exploitation More Likely. Social engineering vector.
P2	CVE-2026-32162	Windows COM	1 week	EoP PR:None local, Exploitation More Likely. Post-exploitation chaining.
P2	CVE-2026-27913	BitLocker	1 week	Secure Boot bypass. Exploitation More Likely. Mobile fleet priority.
P2	CVE-2026-26151	RDP / .rdp	1 week	.rdp phishing — NCSC UK — Likely exploited. Train end users.
P3	93 remaining EoP CVEs	Various	Standard patch cycle	Deploy within normal maintenance windows.

06 Windows 10 KB5082200 — Changelog

La mise à jour KB5082200 (14 avril 2026) porte Windows 10 au build 19045.7184. Destinée aux environnements Windows 10 Enterprise LTSC et aux organisations inscrites au programme Extended Security Updates (ESU). Aucun problème connu signalé par Microsoft.

SECURITY — Anti-Phishing RDP

New protection against phishing via .rdp files

Remote Desktop now displays all requested connection settings before connecting, each parameter disabled by default. One-time warning on first .rdp file open per device. Related to CVE-2026-26151.

SECURITY — Secure Boot

Dynamic Secure Boot status reporting in Windows Security

Secure Boot status tracking via Settings → Windows Security (disabled by default on commercial devices and servers). Fix for BitLocker Recovery bug triggered by Secure Boot updates (Intel Connected Standby devices). Progressive rollout of new Secure Boot certificates replacing 2011 certificates expiring in June 2026.

FIX — Authentication

Microsoft Account sign-in fix (regression since March 2026)

Fix for the "no Internet" error during Microsoft Account authentication introduced since March 2026. Impact: Microsoft Teams, Microsoft Account apps, Microsoft cloud services.

07 Third-Party Security Updates — April 2026

Adobe	**⚠ Zero-Day Acrobat Reader — CVE-2026-34621 (EXPMON)** Patches for Illustrator, Acrobat/Reader, Photoshop, ColdFusion, AEM, InDesign. Emergency fix for actively exploited Reader/Acrobat zero-day detected via EXPMON platform.
Apache	**⚠ RCE ActiveMQ Classic — Undetected for 13 years** Fix for an RCE in Apache ActiveMQ Classic undetected for 13 years. Massively deployed in enterprise Java middleware.
Apple	**DarkSword exploit kit — iOS 18** Extended security updates protecting against the DarkSword exploit kit to more iPhone models running iOS 18.
Cisco	**Auth bypass IMC → Admin** Authentication bypass on the Integrated Management Controller (IMC) enabling Admin access. Targets Cisco UCS out-of-band management.
Fortinet	**⚠ CVE-2026-35616 — FortiClient EMS exploited** Critical vulnerability in FortiClient EMS actively exploited in the wild. Patches released for multiple Fortinet products.
Google	**⚠ Chrome Zero-Day exploited**

	Android April 2026 security bulletin and fix for a Chrome zero-day actively exploited in the wild.
SAP	**Critical SQL Injection — BPC / BW** Critical SQL Injection in SAP Business Planning and Consolidation and SAP Business Warehouse — critical enterprise financial systems.
wolfSSL	**Forged certificates accepted** Flaw in the wolfSSL SSL/TLS library forcing acceptance of forged certificates. Impacts IoT and embedded systems.
GPUBreach	**GPU Rowhammer → full system compromise** New rowhammer attack targeting GPUs enabling privilege escalation and full system compromise.
Marimo	**Pre-auth RCE exploited** Security update for a pre-authentication RCE now actively exploited in the wild.

08 Sources

(1) **Microsoft April 2026 Patch Tuesday fixes 167 flaws, 2 zero-days — BleepingComputer —** https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2026-patch-tuesday-fixes-167-flaws-2-zero-days/

(2) **Microsoft's April 2026 Patch Tuesday Addresses 163 CVEs — Tenable Research —** https://www.tenable.com/blog/microsofts-april-2026-patch-tuesday-addresses-163-cves

(3) **Microsoft releases Windows 10 KB5082200 extended security update — BleepingComputer —** https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-windows-10-kb5082200-extended-security-update/

(4) **Microsoft Security Update Guide — April 2026 — MSRC —** https://msrc.microsoft.com/update-guide/releaseNote/2026-Apr