مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Microsoft Security Updates – April 2026

Tracking #:432318789

Date:15-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft released its April 2026 Patch Tuesday updates, remediating 167 security vulnerabilities across its ecosystem. This release is particularly critical due to the presence of an actively exploited zero-day vulnerability (CVE-2026-32201) affecting Microsoft SharePoint Server.

TECHNICAL DETAILS:

Microsoft released its April 2026 Patch Tuesday updates, remediating 167 security vulnerabilities across its ecosystem. This release is particularly critical due to the presence of an actively exploited zero-day vulnerability (CVE-2026-32201) affecting Microsoft SharePoint Server.

Key risk highlights:

- Multiple unauthenticated Remote Code Execution (RCE) vulnerabilities affecting network services (TCP/IP, IKEv2)
- Client-side attack vectors via Remote Desktop and Microsoft Office
- One vulnerability actively exploited in the wild (SharePoint – CVE-2026-32201)
- High concentration of Elevation of Privilege (EoP) vulnerabilities enabling post-compromise escalation
- Security feature bypasses affecting BitLocker, Secure Boot, and Windows Hello

1. **Actively Exploited Zero-Day**
   - **CVE-2026-32201**
     - **Type:** Spoofing Vulnerability
     - **Affected Product:** Microsoft SharePoint Server
     - **Severity:** Critical (Zero-Day, Exploited in the wild)

Critical Vulnerabilities (High Priority)

- CVE-2026-33824 — Windows IKEv2 RCE
- CVE-2026-33827 — Windows TCP/IP RCE
- CVE-2026-33826 — Active Directory RCE
- CVE-2026-32157 — Remote Desktop Client RCE
- CVE-2026-32190 / 33114 / 33115 — Microsoft Office RCE cluster
- CVE-2026-23666 — .NET DoS

Elevation of Privilege (EoP)

- CVE-2026-26173 / 26177 / 26182 / 27922 — WinSock Driver
- CVE-2026-32070 — CLFS Driver
- CVE-2026-32075 — UPnP Device Host
- CVE-2026-32093 — Function Discovery
- CVE-2026-32152 / 32154 / 32155 — Desktop Window Manager
- CVE-2026-32162 — Windows COM
- CVE-2026-27908 / 27921 — TDI Driver

Security Feature Bypass

- CVE-2026-0390 — UEFI Secure Boot

- CVE-2026-27906 — Windows Hello
- CVE-2026-27913 — BitLocker

Spoofing Vulnerabilities

- CVE-2026-26151 — RDP Spoofing
- CVE-2026-32202 — Windows Shell Spoofing
- CVE-2026-32225 — Shell Security Bypass

RECOMMENDATIONS:

- Patch all systems with April 2026 updates immediately.
- Prioritize:
  - Public-facing SharePoint servers
  - Internet-exposed services
  - Isolate or restrict access to vulnerable SharePoint instances

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2026-Apr