EnCyb

Severity: Critical

Advisory Type: Security

Microsoft Jan 2026 Patch Advisory

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Microsoft's January 2026 Patch Tuesday fixes 114 vulnerabilities, including three zero-days and multiple critical RCE and elevation-of-privilege flaws. Organizations should urgently prioritize zero-days, LSASS, SMB, internet-facing services, and Office to reduce exploitation risk.

- Active Region: Global
- Affected Sector: All sectors using Windows and Microsoft Office, including enterprise IT and developer environments.
- Affected Product: Microsoft Windows, Microsoft Office (Word, Excel), SharePoint Server, Azure components
- Severity: Critical - including three zero-days.
- Published Date: January 14, 2026

CVE DETAILS

CVE	CVE Title	Severity	Impact
CVE-2026-20822	Windows Graphics Component EOP Vulnerability	Critical	EOP
CVE-2026-20876	Windows VBS Enclave EOP Vulnerability	Critical	EOP
CVE-2026-20944	Microsoft Word RCE Vulnerability	Critical	RCE
CVE-2026-20953	Microsoft Office RCE Vulnerability	Critical	RCE
CVE-2026-20955	Microsoft Excel RCE Vulnerability	Critical	RCE
CVE-2026-20854	Windows LSASS RCE Vulnerability	Critical	RCE
CVE-2026-20952	Microsoft Office RCE Vulnerability	Critical	RCE

CVE-2026-20957	Microsoft Excel RCE Vulnerability	Critical	RCE
CVE-2026-20962	DRTM Information Disclosure Vulnerability	Important	InfoDisc
CVE-2026-21265	Secure Boot Certificate Expiration Vulnerability	Zero-day	SecBypass
CVE-2026-0386	Windows Deployment Services RCE Vulnerability	Important	RCE
CVE-2026-20803	Microsoft SQL Server EOP Vulnerability	Important	EOP
CVE-2026-20965	Windows Admin Center EOP Vulnerability	Important	EOP
CVE-2026-20804	Windows Hello Tampering Vulnerability	Important	Tampering
CVE-2026-20805	Desktop Window Manager Info Disclosure Vulnerability	Zero-day	InfoDisc
CVE-2026-20808	Windows File Explorer EOP Vulnerability	Important	EOP
CVE-2026-20809	Windows Kernel Memory EOP Vulnerability	Important	EOP
CVE-2026-20810	WinSock AFD EOP Vulnerability	Important	EOP
CVE-2026-20811	Win32k EOP Vulnerability	Important	EOP
CVE-2026-20812	LDAP Tampering Vulnerability	Important	Tampering
CVE-2026-20814	DirectX Graphics Kernel EOP Vulnerability	Important	EOP
CVE-2026-20815	camsvc EOP Vulnerability	Important	EOP

CVE-2026-20816	Windows Installer EOP Vulnerability	Important	EOP
CVE-2026-20817	Windows Error Reporting EOP Vulnerability	Important	EOP
CVE-2026-20818	Windows Kernel Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20819	Windows VBS Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20820	CLFS Driver EOP Vulnerability	Important	EOP
CVE-2026-20821	RPC Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20823	Windows File Explorer Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20824	Windows Remote Assistance Vulnerability	Important	SecBypass
CVE-2026-20825	Windows Hyper-V Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20826	TWINUI Subsystem Vulnerability	Important	EOP
CVE-2026-20827	TWINUI Subsystem Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20828	rndismp6.sys Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20829	TPM Trustlet Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20831	WinSock AFD EOP Vulnerability	Important	EOP
CVE-2026-20832	RPC IDL EOP Vulnerability	Important	EOP

CVE-2026-20833	Windows Kerberos Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20834	Windows Spoofing Vulnerability	Important	Spoof
CVE-2026-20835	camsvc Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20836	DirectX Graphics Kernel EOP Vulnerability	Important	EOP
CVE-2026-20837	Windows Media RCE Vulnerability	Important	RCE
CVE-2026-20838	Windows Kernel Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20839	CSC Service Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20840	Windows NTFS RCE Vulnerability	Important	RCE
CVE-2026-20842	DWM Core Library EOP Vulnerability	Important	EOP
CVE-2026-20844	Windows Clipboard Server EOP Vulnerability	Important	EOP
CVE-2023-31096	Agere Soft Modem Driver EOP Vulnerability	Zero-day	EOP
CVE-2026-20847	Windows File Explorer Spoofing Vulnerability	Important	Spoof
CVE-2026-20851	camsvc Info Disclosure Vulnerability	Important	InfoDisc
CVE-2026-20852	Windows Hello Tampering Vulnerability	Important	Tampering
CVE-2026-20856	WSUS RCE Vulnerability	Critical	RCE

CVE-2026-20857	Cloud Files Mini Filter Driver EOP Vulnerability	Important	EOP
CVE-2026-20859	Windows Kernel-Mode Driver EOP Vulnerability	Important	EOP
CVE-2026-20875	Windows LSASS DoS Vulnerability	Important	DoS
CVE-2026-20919	Windows SMB Server EOP Vulnerability	Important	EOP
CVE-2026-20922	Windows NTFS RCE Vulnerability	Important	RCE
CVE-2026-20927	Windows SMB Server DoS Vulnerability	Important	DoS
CVE-2026-20929	Windows HTTP.sys EOP Vulnerability	Important	EOP
CVE-2026-20947	Microsoft SharePoint Server RCE Vulnerability	Critical	RCE
CVE-2026-20956	Microsoft SharePoint RCE Vulnerability	Critical	RCE
CVE-2026-21226	Azure Core Python Client Library RCE Vulnerability	Important	RCE

TECHNICAL DETAILS – ZERO-DAY VULNERABILITIES

CVE-2026-20805 – Desktop Window Manager (DWM) Information DisclosureRCE

- **Attack Vector:** Local interaction with Desktop Window Manager through crafted window objects or rendering requests.
- **Cause:** Improper handling of memory references within DWM results in disclosure of uninitialized or previously freed memory regions.
- **Prerequisite:** Local code execution or the ability to trigger window rendering operations under the victim's session.
- **Risk:** Allows attackers to read sensitive memory contents, including pointers, handles, or security-relevant data that can be leveraged to bypass exploit mitigations (ASLR, KASLR) and strengthen follow-on exploitation.

CVE-2026-21265 – Secure Boot Certificate Expiration / Windows Digital Media EoP

- **Attack Vector:** Local exploitation of certificate validation logic within Windows Digital Media and Secure Boot trust chains.
- **Cause:** Inadequate enforcement of certificate expiration checks allows expired or improperly validated certificates to be trusted.
- **Prerequisite:** Attacker must already have local access or code execution on the target system.
- **Risk:** Enables elevation of privilege by subverting trust boundaries, commonly used as a secondary-stage exploit to escalate from user-level access to higher privileges in chained attack scenarios.

CVE-2023-31096 – Legacy Modem Driver Elevation of Privilege

- **Attack Vector:** Local interaction with a legacy Agere/Motorola soft modem kernel-mode driver.
- **Cause:** Improper input validation in driver IOCTL handling permits memory corruption or unauthorized kernel memory access.
- **Prerequisite:** Local access with the ability to load or interact with the vulnerable driver.
- **Risk**: Enables elevation to SYSTEM-level privileges; notable as a “resurfaced” vulnerability where additional exploitation vectors were identified, prompting inclusion in January 2026 cumulative updates.

RECOMMENDATIONS

- Patch zero-day vulnerabilities immediately across all supported systems. Kindly refer the update page: **Microsoft Updates**
- Prioritize LSASS, SMB, WSUS, NTFS, and other internet-facing services
- Update Microsoft Office applications on all endpoints without delay
- Apply patches first to high-privilege and externally exposed systems
- Test updates briefly in staging environments to avoid driver or kernel issues
- Enforce ASR rules and exploit mitigation controls where available
- Track CISA KEV and threat intelligence for signs of rapid exploitation.

REFRENCE

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

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com