مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Microsoft January 2026 Security Updates

Tracking #:432318248

Date:14-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft's January 2026 Patch Tuesday addresses 112–115 security vulnerabilities across Windows including an actively exploited vulnerability in the wild.

TECHNICAL DETAILS:

Microsoft's January 2026 Patch Tuesday addresses 112–115 security vulnerabilities across Windows, Microsoft Office, and related components, including 8 critical vulnerabilities and 3 zero-day issues. Notably, CVE-2026-20805 is confirmed as actively exploited in the wild.

Vulnerability Landscape Overview

- **Total vulnerabilities fixed:** 112–115
- **Critical:** 8
- **Important:** 104–106
- **Zero-days:** 3 (1 exploited, 2 publicly disclosed)

Detailed Vulnerability Analysis

1. Zero-Day Vulnerabilities

- **CVE-2026-20805 – Desktop Window Manager (DWM) Information Disclosure**
  - Severity: Important (CVSS 3.1: 5.5)
  - Exploited in the wild
  - Allows local disclosure of user-mode memory via ALPC port
- **CVE-2023-31096 – Agere Soft Modem Driver Elevation of Privilege**
  - Third-party driver shipped with Windows
  - Exploitation grants **SYSTEM privileges**
  - Mitigation: Removal of agrsm.sys and agrsm64.sys
- **CVE-2026-21265 – Secure Boot Certificate Expiration Bypass**
  - Allows Secure Boot bypass if systems are not updated
  - Root cause: Expiring 2011 Secure Boot certificates
  - High long-term risk for unpatched systems

2. Critical Severity Vulnerabilities

Elevation of Privilege (EoP)

- **CVE-2026-20822 – Windows Graphics Component**
  - Use-after-free vulnerability
  - Local authenticated attacker → SYSTEM privileges
  - CVSS: 7.8
  - Exploitation requires winning a race condition
- **CVE-2026-20876 – Windows VBS Enclave**
  - Heap-based buffer overflow
  - Grants **Virtual Trust Level 2 (VTL2)** privileges
  - CVSS: 6.7

Remote Code Execution (RCE)

- **CVE-2026-20854 – Windows LSASS**
  - Use-after-free vulnerability
  - Network-based RCE without elevated privileges

  - CVSS: 7.5
  - High impact due to credential handling role of LSASS
- **CVE-2026-20944 – Microsoft Word**
  - Out-of-bounds read
  - Exploitable via malicious document
  - CVSS: 7.8
- **CVE-2026-20952 & CVE-2026-20953 – Microsoft Office**
  - Use-after-free vulnerabilities
  - Malicious document or application execution required
  - CVSS: 8.4
- **CVE-2026-20955 – Microsoft Excel**
  - Untrusted pointer reference
  - CVSS: 7.8
- **CVE-2026-20957 – Microsoft Excel**
  - Integer underflow
  - CVSS: 7.8

3. Important Vulnerabilities with Higher Exploitation Likelihood
Microsoft and Cisco Talos highlight the following as **"more likely to be exploited"**:

- **CVE-2026-20816** – Windows Installer EoP
- **CVE-2026-20817** – Windows Error Reporting Service EoP
- **CVE-2026-20820** – Windows CLFS Driver EoP (heap overflow)
- **CVE-2026-20840** – Windows NTFS RCE
- **CVE-2026-20922** – Windows NTFS RCE
- **CVE-2026-20843** – Windows RRAS EoP
- **CVE-2026-20860** – WinSock Ancillary Function Driver EoP
- **CVE-2026-20871** – Desktop Window Manager EoP

RECOMMENDATIONS:

- Deploy January 2026 cumulative updates across all Windows and Office systems.
- Prioritize remediation of CVE-2026-20805.

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-jan