

# Weekly Intelligence Summary

Report Date: 16.02.2026

Intelligence Cut-off Date: 13.02.2026

## Weekly Focus: Patch Tuesday February 2026: Exploited Zero-Days Take Priority

### Active exploitation of Windows security feature bypass and elevation-of-privilege flaws raises enterprise risk

This month's Patch Tuesday from Microsoft delivered 58 security fixes across Windows components and services, including six vulnerabilities confirmed as actively exploited in the wild, several of which were publicly disclosed before patch release. Although the overall number of vulnerabilities is moderate compared to recent months, the presence of multiple exploited zero-days makes this update cycle particularly important for organisations to prioritise.

Among the most significant issues addressed are security feature bypass vulnerabilities affecting Windows Shell, MSHTML, and Microsoft Word, which could allow attackers to circumvent built-in protections such as SmartScreen and OLE safeguards. These vulnerabilities typically require user interaction, such as opening a malicious document, clicking a crafted link, or launching a shortcut file, reinforcing the continued effectiveness of phishing and social-engineering techniques as initial access vectors.

The update also resolves several elevation-of-privilege vulnerabilities in components, including Desktop Window Manager and Remote Desktop Services, which could allow attackers with limited access to escalate privileges to SYSTEM level. Privilege-escalation flaws are frequently used in real-world intrusions to expand control after an initial compromise, making them particularly valuable in multi-stage attack chains. Another actively exploited vulnerability in the Windows Remote Access Connection Manager highlights how even moderate-severity issues can be leveraged once attackers gain a foothold.

### Why It Matters...

February's Patch Tuesday highlights the importance of timely patching and defence-in-depth monitoring. Rather than relying solely on remote code execution vulnerabilities, attackers continue to focus on bypassing security controls and escalating privileges after initial access is obtained. The fact that multiple zero-days were already being exploited demonstrates how quickly threat actors incorporate newly discovered weaknesses into their operations.

Organisations should treat this update cycle as a high priority, ensuring systems are patched promptly, particularly user endpoints, Remote Desktop-enabled systems, and administrative workstations. In parallel, security teams should continue monitoring for suspicious Office activity, SmartScreen bypass attempts, abnormal privilege escalation behaviour, and unusual process execution patterns.

## Intelligence Overview

### Vulnerabilities

[CVE-2026-21643](#) (OVSS: 69 | CVSS: 9.8), a [critical SQL injection vulnerability identified in Fortinet's FortiClient Enterprise Management Server \(EMS\) version 7.4.4](#), could enable the full compromise of the EMS server, access to endpoint data and lateral movement within enterprise networks.

[CVE-2026-25049](#) (OVSS: 72 | CVSS: 9.9), a [critical remote code execution vulnerability in the n8n workflow automation platform](#), could enable full compromise of the n8n server, data exfiltration, credential theft and persistent access.

[CVE-2026-1731](#) (OVSS: 64 | CVSS: 9.9), an [actively exploited critical pre-authentication remote code execution vulnerability in BeyondTrust Remote Support \(RS\) and older versions of Privileged Remote Access \(PRA\)](#), enables full infrastructure compromise, exfiltration of sensitive data and service disruption

[CVE-2026-0229](#) (OVSS: 49 | CVSS 6.6), a [Denial-of-Service \(DoS\) vulnerability in firewalls running PAN-OS from Palo Alto Networks](#), could enable a sustained Denial-of-Service condition by a repeated crash-and-reboot of a firewall.

### Data Breaches

Threat actor using the moniker [w1kkid](#) claimed the [exfiltration of 662,752 Substack account records](#), including email addresses, phone numbers, Stripe IDs and other metadata. Substack confirmed the intrusion.