

Microsoft SharePoint Code Injection Vulnerability Requires Immediate Patching



Microsoft SharePoint contains a code injection vulnerability allowing authorized attackers to execute code remotely over a network, requiring immediate application of vendor security updates.

- CVE-2026-65660 affects Microsoft SharePoint and permits code injection by authorized attackers over a network
- The vulnerability enables remote code execution, posing significant risk to SharePoint deployments
- Organizations must apply vendor-supplied mitigations immediately or discontinue product use if patches are unavailable
- Institutions should evaluate internet exposure of affected assets and prioritize patching based on risk

- Cloud service deployments require specific attention to applicable security update guidance

Vulnerability Overview

Microsoft SharePoint is affected by a **code injection vulnerability** tracked as CVE-2026-65660. The flaw permits an authorized attacker to execute arbitrary code over a network connection, presenting a serious threat to organizations relying on SharePoint for collaboration and document management. The vulnerability requires the attacker to have authorized access, suggesting exploitation could occur through compromised credentials or insider threats.

Risk to Saudi Institutions

SharePoint deployments are widespread across regulated institutions in the Kingdom, including financial services, healthcare, and government entities. The ability to execute code remotely means attackers could potentially access sensitive data, modify critical business information, or establish persistent access within the environment. Organizations using SharePoint in cloud configurations or on-premises installations are both at risk and must assess their specific deployment models.

Remediation Guidance

Microsoft has released security updates to address this vulnerability. Organizations must apply vendor-supplied patches immediately in accordance with their change management procedures. For cloud-based SharePoint deployments, institutions should verify that their service provider has applied necessary updates. If mitigations are not available for specific configurations, organizations should evaluate discontinuing use of affected instances until patches become available. All affected assets should be inventoried, with particular attention to those with internet exposure, and patching should be prioritized based on risk assessment and business criticality.

What to do now

1. Inventory all Microsoft SharePoint instances across the organization, including cloud and on-premises deployments
2. Apply Microsoft security updates for CVE-2026-65660 immediately following change management procedures
3. For cloud SharePoint deployments, verify with service providers that patches have been applied
4. Assess internet exposure of all SharePoint assets and prioritize patching based on risk and business criticality
5. Review access logs for SharePoint environments to detect any suspicious activity by authorized users
6. If patches are unavailable for specific configurations, evaluate temporary isolation or discontinuation of affected instances until mitigations are available