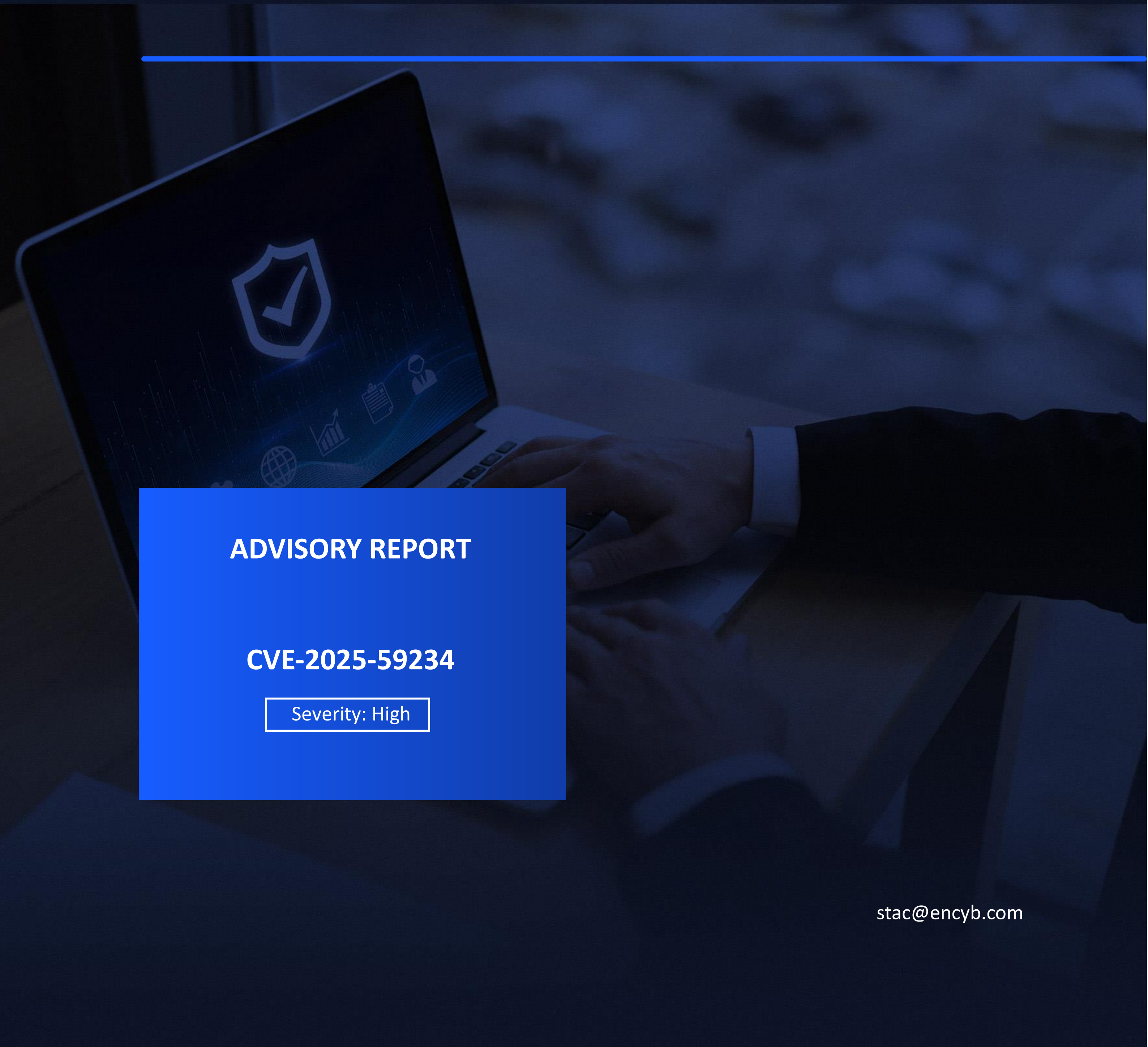
EnCyb

SECURITY THREAT ADVISORY COUNCIL (STAC)

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



ADVISORY REPORT

CVE-2025-59234

Severity: High

stac@encyb.com

OVERVIEW

CVE-2025-59234 is a high-severity “use-after-free” vulnerability (CWE-416) in Microsoft Office that allows a local attacker to execute code. It affects Office 2016, 2019, LTSC 2021/2024, Microsoft 365 Apps, Office for Mac (2021/2024), and Office for Android, with a CVSS 3.1 score of 7.8. Exploitation is considered less likely, and Microsoft has released official patches.

AFFECTED SYSTEMS

- Microsoft Office 2016 (32-bit and x64) versions 16.0.0 before 16.0.5522.1000
- Microsoft Office 2019 (32-bit and x64) versions 19.0.0 before latest security updates
- Microsoft 365 Apps for Enterprise (32-bit and x64) versions 16.0.1 before latest security updates
- Microsoft Office LTSC 2021 (32-bit and x64) versions 16.0.1 before latest security updates
- Microsoft Office LTSC 2024 (32-bit and x64) versions 16.0.0 before latest security updates
- Microsoft Office LTSC for Mac 2021 versions 16.0.1 before 16.102.25101223
- Microsoft Office LTSC for Mac 2024 versions 16.0.0 before 16.102.25101223
- Microsoft Office for Android versions 16.0.1 before 16.0.19328.20000

TECHNICAL DETAILS

- Initial Access: Victim receives a crafted Office document (phishing, malicious download, or shared link).
- Payload Delivery: Opening or previewing the document triggers the Use-After-Free in Office’s parser/renderer.
- Execution: Memory corruption enables arbitrary code execution under the logged-in user.
- Persistence: Attacker may install a service/agent, create scheduled tasks, register add-ins, or add startup registry entries.
- Propagation: Payloads (ransomware/worms) can move via SMB/network shares, email, or cloud-sync.
- Lateral Movement: Stolen credentials or harvested tokens are used to access other hosts, servers, or management interfaces.
- Defence Evasion: Techniques include macro/document obfuscation, exploiting Preview Pane, DLL side-loading, and living-off-the-land.
- Credential Access: Keylogging, memory scraping, and cached credential dumping are common post-compromise steps.
- Discovery: Attacker enumerates drives, services, installed software, domain info, and accessible accounts to identify targets.
- Data Exfiltration: Sensitive files are staged (compressed/encrypted) and exfiltrated over HTTPS/DNS/cloud or C2 channels.
- Command & Control: Malware typically establishes persistent C2 to receive commands, fetch tools, and exfiltrate data.

IMPACT

- Unauthorized access to sensitive files, emails, and credential stores, potentially exposing confidential or proprietary information.
- Ability to modify, corrupt, or falsify critical data, affecting integrity and reliability of systems and records.
- Disruption of system availability, including potential deployment of ransomware, destructive malware, or denial-of-service actions.
- Escalation of privileges and lateral movement across the network, compromising additional hosts, servers, or domain controllers.
- Persistent access through backdoors, scheduled tasks, or malicious Office add-ins, allowing long-term exploitation of the environment.
- Significant financial impact from incident response, system downtime, data recovery, and potential regulatory fines.
- Reputational damage and legal exposure due to breach of sensitive information, affecting customer trust and compliance obligations.
- Difficulty in detection due to obfuscated payloads, living-off-the-land techniques, and command-and-control traffic blending with normal network activity.
- Potential widespread impact across organizations using affected Microsoft Office versions, increasing risk of coordinated attacks or large-scale compromise.

RECOMMENDATIONS

- Apply the latest Microsoft Office security updates and patches immediately.
- Disable or restrict macros and active content in Office documents by default.
- Implement email filtering and attachment scanning to block malicious documents.
- Train users to recognize phishing attempts and avoid opening untrusted Office files.
- Enforce the principle of least privilege to limit the impact of compromised accounts.
- Enable endpoint protection and advanced threat detection solutions to monitor suspicious activity.
- Regularly back up critical data and ensure backups are stored offline or in immutable storage.
- Conduct periodic vulnerability assessments and penetration tests to identify unpatched systems.
- Use multi-factor authentication (MFA) for all user accounts to reduce risk of lateral movement.

REFRENCES

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59234