Your IT Company

Vulnerabilidade crítica de execução remota de código no Microsoft Office (CVE-2026-26110)

ÍNDICE

1. Descrição da vulnerabilidade

Foi identificada uma vulnerabilidade crítica de execução remota de código (Remote Code Execution – RCE) no software Microsoft Office, classificada como CVE-2026-26110.

A falha foi divulgada oficialmente em 10 de março de 2026 e recebeu uma pontuação CVSS 8.4, indicando um risco elevado para ambientes corporativos e usuários que utilizam o pacote de produtividade da Microsoft.

A vulnerabilidade é classificada como CWE-843 – Type Confusion, uma falha que ocorre quando um software manipula um recurso utilizando um tipo de dado incorreto ou incompatível. Em cenários desse tipo, o aplicativo aloca um recurso com determinado tipo de dado, mas posteriormente tenta acessá-lo utilizando outro tipo incompatível.

Essa inconsistência pode causar corrupção de memória, permitindo que um invasor manipule o fluxo de execução do programa. Ao explorar essa condição, um atacante pode forçar o aplicativo a executar comandos arbitrários no sistema afetado.

No contexto do Microsoft Office, essa corrupção de memória pode permitir que atores maliciosos executem código malicioso diretamente no sistema comprometido, abrindo caminho para comprometimento completo da máquina afetada.

De acordo com a postagem realizada pelo ator de ameaça, aproximadamente 3 TB de dados corporativos teriam sido exfiltrados da organização. A listagem foi publicada em um repositório utilizado por grupos de ransomware para expor vítimas e pressionar negociações de resgate.

2. Características Técnicas da Vulnerabilidade

A vulnerabilidade apresenta características que aumentam significativamente seu potencial de risco.

Principais métricas técnicas:

- **CVE:** CVE-2026-26110
- **Tipo:** Execução Remota de Código (RCE)
- **CWE:** CWE-843 – Type Confusion
- **Pontuação CVSS:** 8.4 (Alta)
- **Complexidade do ataque:** Baixa
- **Privilégios necessários:** Nenhum
- **Interação do usuário:** Não necessária
- **Impacto:** Alto em confidencialidade, integridade e disponibilidade

Embora o vetor de ataque seja classificado como local, a execução remota de código refere-se à capacidade do atacante de executar código arbitrário no sistema da vítima após obter um ponto inicial de execução local.

Isso significa que o código malicioso precisa ser executado no sistema da vítima, mas não exige interação direta do usuário, o que pode ocorrer por meio de diferentes vetores de ataque.

Um vetor relevante identificado é o Painel de Visualização do Office, que pode ser utilizado como mecanismo para disparar a exploração da vulnerabilidade.

3. Possíveis Cenários de Exploração

Para explorar a vulnerabilidade CVE-2026-26110, um atacante pode inicialmente obter acesso ao sistema alvo por meio de um vetor de comprometimento inicial. Após esse acesso inicial, o exploit pode ser executado localmente para acionar a falha de Type Confusion.

Entre os possíveis cenários de exploração estão:

- implantação silenciosa de payloads maliciosos em sistemas comprometidos
- execução de código arbitrário no sistema da vítima
- instalação de malware persistente
- implantação de ransomware
- roubo de documentos corporativos
- movimentação lateral dentro da rede corporativa

Uma vez explorada com sucesso, a vulnerabilidade pode permitir que o atacante obtenha controle total sobre o sistema afetado, dependendo do contexto de execução do processo do Office.

Isso pode transformar o dispositivo comprometido em um ponto de entrada para ataques mais amplos dentro da rede corporativa.

4. Status Atual da Exploração

Até o momento da divulgação da vulnerabilidade, não há evidências públicas de exploração ativa da falha CVE-2026-26110.

Segundo análises da própria Microsoft, as seguintes condições foram observadas:

- não há exploração registrada em ambiente real (in-the-wild)
- não existe código de exploração funcional comprovado

- a maturidade do exploit é considerada não comprovada

Entretanto, vulnerabilidades críticas divulgadas publicamente frequentemente passam por um processo de engenharia reversa por atores maliciosos, que analisam os patches de segurança para compreender a falha e desenvolver exploits funcionais.

Esse processo pode levar ao surgimento de exploits nas semanas seguintes à divulgação da correção.

Dessa forma, existe risco de que grupos de ransomware ou atores patrocinados por estados passem a explorar a vulnerabilidade futuramente.

5. Versões Afetadas

A vulnerabilidade impacta diversas versões do Microsoft Office e plataformas associadas.

Entre os produtos afetados estão:

- Microsoft 365 Apps for Enterprise (32-bit e 64-bit)
- Microsoft Office 2019 (32-bit e 64-bit)
- Microsoft Office 2016 (32-bit e 64-bit)
- Microsoft Office LTSC 2021
- Microsoft Office LTSC 2024
- Microsoft Office para Android
- Microsoft Office LTSC para macOS

Essas versões podem estar vulneráveis caso não tenham recebido as atualizações de segurança disponibilizadas pela Microsoft.

6. Versões Corrigidas

A Microsoft disponibilizou atualizações de segurança oficiais em 10 de março de 2026, corrigindo a vulnerabilidade CVE-2026-26110.

Entre as versões com correção aplicada estão:

- **Microsoft Office 2016:** build 16.0.5543.1000 ou superior
- **Microsoft Office LTSC para Mac:** build 16.107.26030819 ou superior
- **Microsoft Office para Android:** build 16.0.19822.20000 ou superior

Para ambientes que utilizam Microsoft 365 Apps for Enterprise, a correção foi disponibilizada por meio do canal padrão de atualizações de segurança da plataforma.

7. Mitigação e Medidas de Segurança

Para reduzir o risco de exploração da vulnerabilidade, recomenda-se a adoção imediata das seguintes medidas de segurança.

- **Aplicação de Patches:** organizações devem aplicar imediatamente as atualizações de segurança disponibilizadas pela Microsoft por meio de:
  - Windows Update
  - Microsoft Update
  - sistemas corporativos de gerenciamento de patches
- **Atualizações Automáticas:** habilitar atualizações automáticas em todos os endpoints garante que futuras correções de segurança sejam aplicadas rapidamente, reduzindo janelas de exposição.
- **Monitoramento de Processos do Office:** soluções de segurança devem monitorar atividades anômalas originadas por aplicativos do Office, incluindo:
  - execução de processos suspeitos
  - criação de scripts inesperados
  - atividades incomuns em segundo plano
- **Restrição de Privilégios:** aplicação do princípio de menor privilégio pode limitar o impacto caso um sistema seja comprometido. Usuários devem possuir apenas as permissões necessárias para execução de suas atividades.
- **Uso de Soluções EDR:** Ferramentas de Endpoint Detection and Response (EDR) podem auxiliar na detecção de comportamentos suspeitos relacionados à exploração de vulnerabilidades em aplicativos do Office.

8. Avaliação de Risco

A vulnerabilidade CVE-2026-26110 apresenta características que a tornam particularmente relevante para ambientes corporativos. Fatores que aumentam o risco incluem:

- baixa complexidade de exploração
- ausência de necessidade de privilégios
- ausência de interação do usuário
- amplo uso do Microsoft Office em ambientes corporativos

Embora não existam evidências atuais de exploração ativa, vulnerabilidades críticas em softwares amplamente utilizados tendem a se tornar alvo de exploração rapidamente após a divulgação pública.

Portanto, organizações devem tratar essa vulnerabilidade como prioridade alta de remediação, especialmente em ambientes corporativos que dependem intensivamente do pacote Microsoft Office para atividades operacionais.

9. Referências Técnicas

Para saber informações mais detalhadas sobre este tema, acesse:

- https://gbhackers.com/critical-vulnerability-in-microsoft-office/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26110

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Equipe de Threat Intelligence