Patches críticos emitidos para produtos da Microsoft, 09 de setembro de 2

Data: 2025-09-12 06:41:06

Autor: Inteligência Against Invaders

NÚMERO DO AVISO MS-ISAC:

2025-082

DATA(S) DE EMISSÃO:

09/09/2025

VISÃO GERAL:

Várias vulnerabilidades foram descobertas em produtos da Microsoft, a mais grave das quais pode permitir a execução remota de código. A exploração bem-sucedida da mais grave dessas vulnerabilidades pode resultar em um invasor obtendo os mesmos privilégios que o usuário conectado. Dependendo dos privilégios associados ao usuário, um invasor pode instalar programas; visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário. Os usuários cujas contas estão configuradas para ter menos direitos de usuário no sistema podem ser menos afetados do que aqueles que operam com direitos de usuário administrativos.

INTELIGÊNCIA DE AMEAÇAS:

Atualmente, não há relatos dessas vulnerabilidades sendo exploradas na natureza.

SISTEMAS AFETADOS:

- Servidor SQL
- Agente de Máquina Virtual do Windows do Azure
- Windows PowerShell
- Microsoft Edge (baseado em Chromium)
- RRAS (Serviço de Roteamento e Acesso Remoto) do Windows
- Componente de imagem do Windows
- Componente do Microsoft Graphics
- Windows DWM
- Serviço Bluetooth do Windows
- Windows Kernel
- Serviços de Informações da Internet do Windows
- Serviço de Firewall do Windows Defender
- Serviço de Subsistema de Autoridade de Segurança Local do Windows (LSASS)
- Função: Windows Hyper-V
- Windows TCP/IP
- Driver de função auxiliar do Windows para WinSock
- Cliente SMBv3 do Windows
- Serviço de Plataforma de Dispositivos Conectados do Windows
- Serviços de Gerenciamento do Windows
- Sistema de arquivos de intermediação da Microsoft
- Windows MapUrlToZone
- Serviço de Gerenciamento de Acesso por Funcionalidade (camsvc)
- Windows interface do usuário XAML Phone DatePickerFlyout
- Disco rígido virtual da Microsoft
- Serviços do Windows MultiPoint
- Negociação estendida do Windows SPNEGO
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Escritório da Microsoft
- Microsoft Office Visio
- Microsoft Office PowerPoint
- Windows BitLocker
- Mapas XAML da interface do usuário do Windows MapControlSettings
- Windows NTFS
- Windows NTLM
- Windows Win32K – GRFX
- Kernel gráfico
- Pacote de computação de alto desempenho (HPC) da Microsoft
- Windows SMB

RISCO:

Governo:

Grandes e médias entidades governamentaisALTO

Governo pequenoMÉDIA

Empresas:

Entidades de grandes e médias empresasALTO

Entidades de pequenas empresasMÉDIA

RESUMO TÉCNICO:

Várias vulnerabilidades foram descobertas em produtos da Microsoft, a mais grave das quais pode permitir a execução remota de código.

Uma lista completa de todas as vulnerabilidades pode ser encontrada no link da Microsoft na seção Referência.

A exploração bem-sucedida da mais grave dessas vulnerabilidades pode resultar em um invasor obtendo os mesmos privilégios que o usuário conectado. Dependendo dos privilégios associados ao usuário, um invasor pode instalar programas; visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário. Os usuários cujas contas estão configuradas para ter menos direitos de usuário no sistema podem ser menos afetados do que aqueles que operam com direitos de usuário administrativos.

RECOMENDAÇÕES:

Recomendamos que as seguintes ações sejam tomadas:

- Aplique as atualizações apropriadas fornecidas pela Microsoft aos sistemas vulneráveis imediatamente após o teste apropriado. (**M1051: Atualizar software**)

- **Salvaguarda 7.1: Estabelecer e manter um processo de gerenciamento de vulnerabilidades:** Estabeleça e mantenha um processo documentado de gerenciamento de vulnerabilidades para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda.
- **Salvaguarda 7.2: Estabelecer e manter um processo de correção:**Estabeleça e mantenha uma estratégia de correção baseada em risco documentada em um processo de correção, com revisões mensais ou mais frequentes.
- **Safeguard 7.4: Execute o gerenciamento automatizado de patches de aplicativos:**Execute atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência.
- **Safeguard 7.5: Execute verificações automatizadas de vulnerabilidades de ativos corporativos internos:** Execute verificações automatizadas de vulnerabilidades da empresa interna ativos em uma base trimestral, ou mais frequente. Realize verificações autenticadas e não autenticadas, usando uma ferramenta de verificação de vulnerabilidades compatível com SCAP.
- **Salvaguarda 7.7: Corrigir vulnerabilidades detectadas:**Corrija vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente ou com mais frequência, com base no processo de correção.
- **Salvaguarda 12.1: Garantir que a infraestrutura de rede esteja atualizada:**Certifique-se de que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de rede como serviço (NaaS) com suporte no momento. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte ao software.
- **Salvaguarda 18.1: Estabelecer e manter um programa de teste de penetração:**Estabelecer e manter um programa de teste de penetração apropriado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de penetração incluem escopo, como rede, aplicativo Web, Interface de Programação de Aplicativos (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações de ponto de contato; correção, como a forma como as descobertas serão roteadas internamente; e requisitos retrospectivos.
- **Salvaguarda 18.2: Executar testes periódicos de penetração externa:**Realize testes periódicos de penetração externa com base nos requisitos do programa, pelo menos anualmente. O teste de penetração externa deve incluir reconhecimento corporativo e ambiental para detectar informações exploráveis. O teste de penetração requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser uma caixa transparente ou uma caixa opaca.
- **Salvaguarda 18.3: Corrigir resultados do teste de penetração:**Corrija as descobertas do teste de penetração com base na política da empresa para escopo e priorização de correção.
- Aplique o Princípio do Menor Privilégio a todos os sistemas e serviços. Execute todos os softwares como um usuário sem privilégios (sem privilégios administrativos) para diminuir os efeitos de um ataque bem-sucedido. (**M1026: Gerenciamento de contas privilegiadas**)
- **Salvaguarda 4.7: Gerenciar contas padrão em ativos e software corporativos:**Gerencie contas padrão em ativos e software corporativos, como raiz, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desabilitar contas padrão ou torná-las inutilizáveis.
- **Salvaguarda 5.5: Estabelecer e manter um inventário de contas de serviço:**Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter o proprietário do departamento, a data de revisão e a finalidade. Execute revisões de conta de serviço para validar se todas as contas ativas estão autorizadas, em uma agenda recorrente

no mínimo trimestralmente ou com mais frequência.

- A verificação de vulnerabilidades é usada para encontrar vulnerabilidades de software potencialmente exploráveis para corrigi-las. (**M1016**:**Verificação de vulnerabilidades**)
- **Salvaguarda 16.13: Realizar Teste de Penetração de Aplicativos:**Realize testes de penetração de aplicativos. Para aplicativos críticos, o teste de penetração autenticado é mais adequado para encontrar vulnerabilidades de lógica de negócios do que a verificação de código e o teste de segurança automatizado. O teste de penetração depende da habilidade do testador de manipular manualmente um aplicativo como um usuário autenticado e não autenticado.
- Arquitetar seções da rede para isolar sistemas, funções ou recursos críticos. Use segmentação física e lógica para impedir o acesso a sistemas e informações potencialmente confidenciais. Use uma DMZ para conter todos os serviços voltados para a Internet que não devem ser expostos da rede interna. Configure instâncias separadas de nuvem privada virtual (VPC) para isolar sistemas de nuvem críticos. (**M1030**:**Segmentação de rede**)
- **Salvaguarda 12.2: Estabelecer e manter uma arquitetura de rede segura:** Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar a segmentação, o menor privilégio e a disponibilidade, no mínimo.
- Use recursos para detectar e bloquear condições que possam levar ou ser indicativas da ocorrência de uma exploração de software. (**M1050:Proteção contra exploits**)
- **Salvaguarda 10.5:Ative os recursos anti-exploração:**Habilite recursos antiexploração em ativos e software corporativos, sempre que possível, como® Microsoft Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) ou Apple® System InteProteção Grity (SIP) e Gatekeeper™.