O Patch Tuesday de setembro de 2025 da Microsoft corrige 81 falhas, dois

Data: 2025-09-09 17:56:24

Autor: Inteligência Against Invaders

Hoje é o Patch Tuesday de setembro de 2025 da Microsoft, que inclui atualizações de segurança

para 81 falhas, incluindo duas vulnerabilidades de dia zero divulgadas publicamente.

Este Patch Tuesday também corrige nove vulnerabilidades “críticas”, cinco das quais são vulnerabilidades de execução remota de código, 1 é divulgação de informações e 2 são elevação de privilégios.

Quando o BleepingComputer relata as atualizações de segurança do Patch Tuesday, contamos apenas as lançadas no Patch Tuesday.

Portanto, o número de falhas não inclui três vulnerabilidades do Azure, uma do Dynamics 365 FastTrack Implementation Assets, duas do Mariner, cinco do Microsoft Edge e 1 do Xbox corrigidas no início deste mês.

O Patch Tuesday deste mês corrige duas falhas de dia zero divulgadas publicamente no Windows SMB Server e no Microsoft SQL Server. Microsoft classifica uma falha de dia zero como divulgado publicamente ou explorado ativamente enquanto nenhuma correção oficial estiver disponível.

A Microsoft corrigiu uma falha de elevação de privilégios no SMB Server que é explorada por meio de ataques de retransmissão.

“O servidor SMB pode ser suscetível a ataques de retransmissão, dependendo da configuração. Um invasor que explorasse com sucesso essas vulnerabilidades poderia realizar ataques de retransmissão e tornar os usuários sujeitos a ataques de elevação de privilégio”, explica a Microsoft.

Microsoft diz que o Windows já inclui configurações para proteger o servidor SMB contra ataques de retransmissão, incluindo a habilitação da Assinatura de Servidor SMB e da Proteção Estendida para Autenticação (EPA) do Servidor SMB.

No entanto, habilitar esses recursos pode causar problemas de compatibilidade com dispositivos e implementações mais antigos.

A Microsoft recomenda que os administradores habilitem a auditoria em servidores SMB para determinar se encontrarão algum problema quando esses recursos de proteção forem totalmente aplicados.

“Como parte das atualizações do Windows lançadas a partir de 9 de setembro de 2025 (CVE-2025-55234), o suporte está habilitado para auditar a compatibilidade do cliente SMB para assinatura do SMB Server, bem como SMB Server EPA”, explica a Microsoft.

A Microsoft não atribuiu a falha a nenhum pesquisador e não está claro onde ela foi divulgada.

CVE-2024-21907 **-VulnCheck: CVE-2024-21907 Tratamento inadequado de condições excepcionais em Newtonsoft.Json**

A Microsoft corrigiu uma vulnerabilidade anteriormente conhecida emNewtonsoft.Json que está incluído como parte do Microsoft SQL Server.

“O CVE-2024-21907 aborda uma vulnerabilidade de tratamento incorreto de condições excepcionais no Newtonsoft.Json antes da versão 13.0.1”, explica a Microsoft.

“Os dados criados que são passados para o método JsonConvert.DeserializeObject podem acionar uma exceção StackOverflow, resultando em negação de serviço. Dependendo do uso da biblioteca, um invasor remoto e não autenticado pode causar a condição de negação de serviço.”

“As atualizações documentadas do SQL Server incorporam atualizações no Newtonsoft.Json que abordam essa vulnerabilidade.”

Abaixo está a lista completa de vulnerabilidades resolvidas nas atualizações do Patch Tuesday de setembro de 2025.

Para acessar a descrição completa de cada vulnerabilidade e os sistemas que ela afeta, você pode visualizar orelatório completo aqui.

Etiqueta	CVE ID	Título CVE	Severidade
Azure – Rede	CVE-2025-54914	Vulnerabilidade de elevação de privilégio de rede do Azure	Crítico
Azure Arc	CVE-2025-55316	Vulnerabilidade de elevação de privilégio do Azure Arc	Importante
Serviço de Bot do Azure	CVE-2025-55244	Vulnerabilidade de elevação de privilégio do Serviço de Bot do Azure	Crítico
Azure Entra	CVE-2025-55241	Vulnerabilidade de elevação de privilégio do Azure Entra	Crítico
Agente de Máquina Virtual do Windows do Azure	CVE-2025-49692	Vulnerabilidade de elevação de privilégio do agente de máquina conectada do Azure	Importante
Serviço de Gerenciamento de Acesso por Funcionalidade (camsvc)	CVE-2025-54108	Vulnerabilidade de elevação de privilégio do Serviço de Gerenciamento de Acesso por Capacidade (camsvc)	Importante
Ativos de implementação do Dynamics 365 FastTrack	CVE-2025-55238	Vulnerabilidade de divulgação de informações de ativos de implementação do Dynamics 365 FastTrack	Crítico

Kernel gráfico	CVE-2025-55236	Vulnerabilidade de execução remota de código do kernel gráfico	Crítico
Kernel gráfico	CVE-2025-55223	DirectX GVulnerabilidade de elevação de privilégio do kernel raphics	Importante
Kernel gráfico	CVE-2025-55226	Vulnerabilidade de execução remota de código do kernel gráfico	Crítico
Microsoft AutoUpdate (MAU)	CVE-2025-55317	Vulnerabilidade de elevação de privilégio do Microsoft AutoUpdate (MAU)	Importante
Sistema de arquivos de intermediação da Microsoft	CVE-2025-54105	Vulnerabilidade de elevação de privilégio do sistema de arquivos do Microsoft Brokering	Importante
Microsoft Edge (baseado em Chromium)	CVE-2025-9866	Chromium: CVE-2025-9866 Implementação inadequada em extensões	Desconhecido
Microsoft Edge (baseado em Chromium)	CVE-2025-9867	Chromium: CVE-2025-9867 Implementação inadequada em downloads	Desconhecido
Microsoft Edge (baseado em Chromium)	CVE-2025-53791	Vulnerabilidade de desvio do recurso de segurança do Microsoft Edge (baseado em Chromium)	Moderado
Microsoft Edge (baseado em Chromium)	CVE-2025-9864	Chromium: CVE-2025-9864 Use após o free no V8	Desconhecido
Microsoft Edge (baseado em Chromium)	CVE-2025-9865	Chromium: CVE-2025-9865 Implementação inadequada na barra de ferramentas	Desconhecido
Componente do Microsoft Graphics	CVE-2025-53807	Vulnerabilidade de elevação de privilégio do componente gráfico do Windows	Importante
Componente do Microsoft Graphics	CVE-2025-53800	Vulnerabilidade de elevação de privilégio do componente gráfico do Windows	Crítico
Pacote de computação	CVE-2025-55232	Vulnerabilidade de	Importante

de alto desempenho (HPC) da Microsoft		execução remota de código do pacote de computação de alto desempenho (HPC) da Microsoft	
Escritório da Microsoft	CVE-2025-54910	Vulnerabilidade de execução remota de código do Microsoft Office	Crítico
Escritório da Microsoft	CVE-2025-55243	Vulnerabilidade de falsificação do Microsoft OfficePlus	Importante
Escritório da Microsoft	CVE-2025-54906	Vulnerabilidade de execução remota de código do Microsoft Office	Importante
Microsoft Office Excel	CVE-2025-54902	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54899	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54904	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54903	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54898	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54896	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54900	Vulnerabilidade de execução remota de código do Microsoft Excel	Importante
Microsoft Office Excel	CVE-2025-54901	Vulnerabilidade de divulgação não autorizada de informações do Microsoft Excel	Importante
Microsoft Office	CVE-2025-54908	Vulnerabilidade de	Importante

PowerPoint		execução remota de código do Microsoft PowerPoint	
Microsoft Office SharePoint	CVE-2025-54897	Vulnerabilidade de execução remota de código do Microsoft SharePoint	Importante
Microsoft Office Visio	CVE-2025-54907	Vulnerabilidade de execução remota de código do Microsoft Office Visio	Importante
Microsoft Office Word	CVE-2025-54905	Vulnerabilidade de divulgação não autorizada de informações do Microsoft Word	Importante
Disco rígido virtual da Microsoft	CVE-2025-54112	Vulnerabilidade de elevação de privilégio do disco rígido virtual da Microsoft	Importante
Função: Windows Hyper-V	CVE-2025-54092	Vulnerabilidade de elevação de privilégio do Windows Hyper-V	Importante
Função: Windows Hyper-V	CVE-2025-54091	Vulnerabilidade de elevação de privilégio do Windows Hyper-V	Importante
Função: Windows Hyper-V	CVE-2025-54115	Vulnerabilidade de elevação de privilégio do Windows Hyper-V	Importante
Função: Windows Hyper-V	CVE-2025-54098	Vulnerabilidade de elevação de privilégio do Windows Hyper-V	Importante
Servidor SQL	CVE-2025-47997	Vulnerabilidade de divulgação não autorizada de informações do Microsoft SQL Server	Importante
Servidor SQL	CVE-2025-55227	Vulnerabilidade de elevação de privilégio do Microsoft SQL Server	Importante
Servidor SQL	CVE-2024-21907	VulnCheck: CVE-2024-21907 Tratamento inadequado de condições excepcionais em Newtonsoft.Json	Desconhecido
Driver de função auxiliar do Windows para WinSock	CVE-2025-54099	Driver de função auxiliar do Windows para vulnerabilidade de elevação de privilégio	Importante

		WinSock	
Windows BitLocker	CVE-2025-54911	Vulnerabilidade de elevação de privilégio do Windows BitLocker	Importante
Windows BitLocker	CVE-2025-54912	Vulnerabilidade de elevação de privilégio do Windows BitLocker	Importante
Serviço Bluetooth do Windows	CVE-2025-53802	Vulnerabilidade de elevação de privilégio do serviço Bluetooth do Windows	Importante
Serviço de Plataforma de Dispositivos Conectados do Windows	CVE-2025-54102	Vulnerabilidade de elevação de privilégio do serviço Windows Connected Devices Platform	Importante
Serviço de Plataforma de Dispositivos Conectados do Windows	CVE-2025-54114	Vulnerabilidade de negação de serviço do Windows Connected Devices Platform Service (Cdpsvc)	Importante
Serviço de Firewall do Windows Defender	CVE-2025-53810	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Serviço de Firewall do Windows Defender	CVE-2025-53808	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Serviço de Firewall do Windows Defender	CVE-2025-54094	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Serviço de Firewall do Windows Defender	CVE-2025-54915	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Serviço de Firewall do Windows Defender	CVE-2025-54109	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Serviço de Firewall do Windows Defender	CVE-2025-54104	Vulnerabilidade de elevação de privilégio do serviço de Firewall do Windows Defender	Importante
Windows DWM	CVE-2025-53801	Vulnerabilidade de elevação de privilégio da biblioteca principal do Microsoft DWM	Importante
Componente de imagem	CVE-2025-53799	Vulnerabilidade de	Crítico

do Windows		divulgação não autorizada de informações do componente de imagem do Windows	
Serviços de Informações da Internet do Windows	CVE-2025-53805	HTTP.sys Vulnerabilidade de negação de serviço	Importante
Windows Kernel	CVE-2025-53803	Vulnerabilidade de divulgação não autorizada de informações de memória do kernel do Windows	Importante
Windows Kernel	CVE-2025-53804	Vulnerabilidade de divulgação não autorizada de informações do driver do modo kernel do Windows	Importante
Windows Kernel	CVE-2025-54110	Vulnerabilidade de elevação de privilégio do kernel do Windows	Importante
Serviço de Subsistema de Autoridade de Segurança Local do Windows (LSASS)	CVE-2025-54894	Vulnerabilidade de elevação de privilégio do serviço do subsistema da autoridade de segurança local	Importante
Serviço de Subsistema de Autoridade de Segurança Local do Windows (LSASS)	CVE-2025-53809	Vulnerabilidade de negação de serviço do LSASS (Serviço de Subsistema de Autoridade de Segurança Local)	Importante
Serviços de Gerenciamento do Windows	CVE-2025-54103	Vulnerabilidade de elevação de privilégio do Serviço de Gerenciamento do Windows	Importante
Windows MapUrlToZone	CVE-2025-54107	Vulnerabilidade de desvio do recurso de segurança MapUrlToZone	Importante
Windows MapUrlToZone	CVE-2025-54917	Vulnerabilidade de desvio do recurso de segurança MapUrlToZone	Importante
Serviços do Windows MultiPoint	CVE-2025-54116	Vulnerabilidade de elevação de privilégio do Windows MultiPoint Services	Importante

Windows NTFS	CVE-2025-54916	Vulnerabilidade de execução remota de código do Windows NTFS	Importante
Windows NTLM	CVE-2025-54918	Vulnerabilidade de elevação de privilégio do Windows NTLM	Crítico
Windows PowerShell	CVE-2025-49734	Vulnerabilidade de elevação direta de privilégio do PowerShell	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-54095	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-54096	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-53797	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-53796	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-54106	Vulnerabilidade de execução remota de código do RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-54097	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS)	Importante

		do Windows	
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-53798	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-54113	Vulnerabilidade de execução remota de código do RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-55225	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
RRAS (Serviço de Roteamento e Acesso Remoto) do Windows	CVE-2025-53806	Vulnerabilidade de divulgação não autorizada de informações do Serviço de Roteamento e Acesso Remoto (RRAS) do Windows	Importante
Windows SMB	CVE-2025-55234	Vulnerabilidade de elevação de privilégio do Windows SMB	Importante
Cliente SMBv3 do Windows	CVE-2025-54101	Vulnerabilidade de execução remota de código do cliente SMB do Windows	Importante
Negociação estendida do Windows SPNEGO	CVE-2025-54895	Vulnerabilidade de elevação de privilégio do mecanismo de segurança de negociação estendida SPNEGO (NEGOEX)	Importante
Windows TCP/IP	CVE-2025-54093	Vulnerabilidade de elevação de privilégio do driver TCP/IP do Windows	Importante
Mapas XAML da interface do usuário do Windows MapControlSettings	CVE-2025-54913	Vulnerabilidade de elevação de privilégio de mapas XAML da interface do usuário do Windows	Importante

		MapControlSettings	
Windows interface do usuário XAML Phone DatePickerFlyout	CVE-2025-54111	Vulnerabilidade de elevação de privilégio do telefone XAML da interface do usuário do Windows DatePickerFlyout	Importante
Windows Win32K – GRFX	CVE-2025-55224	Vulnerabilidade de execução remota de código do Windows Hyper-V	Crítico
Windows Win32K – GRFX	CVE-2025-55228	Vulnerabilidade de execução remota de código do componente gráfico do Windows	Crítico
Windows Win32K – GRFX	CVE-2025-54919	Vulnerabilidade de execução remota de código do componente gráfico do Windows	Importante
Xboxe	CVE-2025-55242	Vulnerabilidade de divulgação de informações do Djando do Copilot Bug de certificação do Xbox	Crítico
Serviços de jogos XBox	CVE-2025-55245	Vulnerabilidade de elevação de privilégio do Xbox Gaming Services	Importante