Mil CVEs por mês quebram o ciclo mensal de correção, e a saída é decidir a ordem antes de abrir o boletim

O boletim da Microsoft de 10 de novembro trouxe 1.093 CVEs próprias segundo a contagem da Tenable, espalhadas por 287 produtos e componentes, com 63 classificadas como críticas e 1.029 como importantes. O Internet Storm Center do SANS contou 1.260 no total, dos quais 167 são problemas do Chromium que chegam pelo Edge, e Johannes Ullrich batizou o fenômeno de surto de correção induzido por IA. É o segundo mês consecutivo acima de mil. Uma única falha está sendo explorada, a CVE-2026-124194 do Outlook, com nota 6,5 e severidade Moderada, e ela entrou no catálogo de vulnerabilidades exploradas da CISA com prazo federal de 24 de novembro. A combinação de volume recorde com severidade baixa no único item explorado é exatamente o cenário em que a fila por nota falha, e esta análise propõe outra fila.

`1.093 CVEs da Microsoft  /  63 críticas, 1.029 importantes  /  167 CVEs do Chromium no Edge  /  CVE-2026-124194 no catálogo da CISA  /  Prazo federal: 24 de novembro`

O problema desta análise: o ciclo mensal de correção foi desenhado para boletins de dezenas de CVEs e está recebendo boletins de mais de mil. Nenhum time cresceu na mesma proporção. Quando a fila é montada por nota de severidade, o resultado é um mês gasto em elevação de privilégio local enquanto a falha que está sendo usada contra alvos reais fica para depois, porque recebeu 6,5.

- Quatro contagens públicas diferentes para o mesmo boletim, e saber qual delas você está gerenciando muda o indicador que vai ao conselho.
- Dois exemplos deste mês em que a nota engana em direções opostas: 9,9 rotulada como importante e 10,0 que não pede ação do cliente.
- Um método de triagem em quatro perguntas, na ordem em que elas eliminam trabalho.
- A fila concreta de novembro, com os CVEs nomeados, e as medidas de rede que valem mais que o patch no caso do Outlook.

Comece pelo número, porque ele não é um número. São quatro.

Fonte	Contagem	Critério
Tenable	1.093	CVEs atribuídas pela Microsoft, em 287 produtos e componentes
SANS Internet Storm Center	1.260	Total do boletim, incluindo 167 do Chromium que afetam o Edge
The Hacker News	1.259	Total, com 165 CVEs de terceiros destacadas
BleepingComputer	1.235	Contagem própria do veículo

A diferença entre 1.093 e 1.260 é quase inteira o Chromium chegando pelo Edge. Isso não é detalhe de contabilidade. Se o seu parque atualiza o Edge pelo canal do navegador, essas 167 saem da sua fila de servidor antes de você abrir a planilha. Se você reporta ao conselho o número grande e gerencia o número pequeno, o indicador de cobertura vai parecer pior do que é, todo mês.

A distribuição por tipo também importa mais que a severidade. Pela leitura da Tenable, elevação de privilégio responde por cerca de 48,9% do boletim e execução remota de código por cerca de 27,1%. Quase metade do mês é

um degrau que só serve a quem já está dentro.

A única explorada tem nota 6,5

A CVE-2026-124194 é falsificação no Outlook, CVSS 6,5, severidade Moderada no catálogo da Microsoft. O mecanismo: um atacante não autenticado envia um arquivo de mensagem preparado e, ao abri-lo, o Outlook conecta a um local de rede controlado pelo atacante sem exibir o aviso que normalmente aparece para conteúdo externo. O que sai nessa conexão é dado de autenticação, entre ele o hash NTLMv2, que serve para se passar pelo usuário. Exige conectividade de rede e interação do usuário.

A Microsoft diz que a falha foi explorada como dia zero. Não atribuiu a nenhum ator, não publicou detalhe técnico e não esclareceu se a descoberta veio antes ou depois do início da exploração. O crédito é do pesquisador identificado como Nono e de Benoît Sevens, da Anthropic, com uso do Claude na investigação. A CISA incluiu o item no catálogo de vulnerabilidades exploradas conhecidas, com prazo de 24 de novembro para órgãos federais americanos.

Guarde o contraste: Moderada, 6,5, e em exploração ativa num catálogo de obrigação legal. Qualquer processo que ordene a fila por nota vai colocar esse item depois de centenas de outros.

Dois casos em que a nota engana

Não é um acidente isolado deste mês. O mesmo boletim traz os dois erros possíveis.

- Nota alta, risco menor que parece. A CVE-2026-109469, de elevação de privilégio em registro de dispositivo no Entra, aparece como crítica com CVSS 10,0 e com a observação de que não requer ação do cliente. É corrigida no serviço. Entrar na fila do time de infraestrutura com prioridade máxima é desperdiçar a semana.
- Nota menor que o risco. A CVE-2026-120002, elevação de privilégio no SharePoint Server, aparece com CVSS 9,9 e rótulo de importante. O rótulo e o número discordam no mesmo documento.

A conclusão operacional é desconfortável, mas simples: severidade publicada é entrada de informação, não é decisão. A decisão precisa de contexto que só existe dentro da sua organização.

O método em quatro perguntas

A ordem abaixo segue a recomendação que Jake Knott, da watchTowr, resumiu para este boletim, com duas perguntas de contexto que reduzem o volume antes de começar o trabalho. A sequência importa porque cada pergunta descarta itens que a seguinte nem precisa avaliar.

1. Está exposto à internet?

Primeiro o que um estranho alcança sem credencial. Isso separa serviço de borda e de identidade de tudo o mais. Em novembro, essa pergunta puxa para cima a execução remota em Active Directory Domain Services, Exchange Server, LDAP, Schannel, NAT e TCP/IP. É um conjunto pequeno dentro de mil, e é onde a janela de exposição custa mais caro.

2. Está sendo explorado?

Fontes que respondem isso em minutos: o catálogo da CISA, o diário do Internet Storm Center e o próprio aviso do fabricante. Neste mês a resposta é um item. A pergunta nunca devolve uma lista grande, e é por isso que ela cabe antes de qualquer inventário.

3. O componente existe no parque?

Aqui o boletim encolhe de verdade. Os dez produtos com mais CVEs em novembro, pela contagem da Tenable, dão o mapa de onde o esforço vai cair:

Produto	CVEs
Word	65
Excel	64
SQL Server	53
Windows Advanced Rasterization Platform	37
Windows Installer	36
Windows Graphics Kernel	35
Windows Kernel	28
SharePoint	27
Windows DNS	22
Outlook e Print Spooler	20 cada

Quem não tem SQL Server no parque acabou de tirar 53 itens da conta. Quem não roda SharePoint local, outras 27. Esse é o passo que a maioria dos times faz por último, quando devia fazer terceiro.

4. Os pré-requisitos são atingíveis no seu ambiente?

Interação do usuário, conta local já existente, adjacência de rede. Uma elevação de privilégio local em servidor onde ninguém tem sessão interativa e nenhuma aplicação executa código de terceiro é risco diferente da mesma falha em estação de desenvolvedor. A nota é a mesma nos dois casos.

A fila concreta de novembro

Aplicando as quatro perguntas ao boletim deste mês, com os identificadores nomeados:

Prioridade	Itens	Por quê
Imediata	CVE-2026-124194 (Outlook)	Única em exploração, no catálogo da CISA, prazo de 24 de novembro
Esta semana	CVE-2026-118146 (AD DS), CVE-2026-118207 (Exchange), CVE-2026-119958 (LDAP), CVE-2026-119952 (Schannel), CVE-2026-113862 (NAT), CVE-2026-113859 (TCP/IP)	Execução remota em serviço de borda ou de identidade
Esta semana, parque de desenvolvimento	CVE-2026-121662 e CVE-2026-121663 (Visual Studio Code)	Execução de código e contorno de recurso de segurança em estação que guarda credencial e token
Janela normal	Elevações marcadas como exploração mais provável, entre elas Windows Installer, WMI, Kernel, Print Spooler e Winlogon	Degrau de pós-comprometimento, com volume alto e janela tolerável
Fora da fila local	CVE-2026-109469 (Entra) e as 167 do Chromium	Corrigidas no serviço ou pelo canal do navegador

No caso do Outlook, a rede resolve mais rápido que o patch

Distribuir atualização de Office em parque grande leva dias. Fechar a saída que a falha usa leva horas, e vale manter fechada depois do patch.

- Bloquear tráfego SMB e autenticação NTLM saindo para a internet na borda. É o que transforma o vazamento de hash em conexão que não completa.
- Ativar auditoria de NTLM antes de restringir, para medir o que quebraria, e então aplicar restrição por política.
- Colocar conta administrativa no grupo de usuários protegidos, que impede o uso desse tipo de credencial em autenticação NTLM.
- Exigir assinatura de SMB, que reduz o valor do hash capturado em ataque de retransmissão.

Nenhuma dessas quatro medidas depende do calendário da Microsoft, e todas servem para a próxima falha da mesma família, que vai existir.

Três números para levar ao conselho

Relatório de correção que lista quantidade de patch aplicado não informa risco. Três indicadores informam:

- Cobertura do parque por componente. Percentual de máquinas com a versão corrigida, por produto, e não por total de CVEs fechadas. É o único jeito de responder se o Outlook foi corrigido.
- Prazo até a correção do que está exposto. Tempo médio entre publicação do boletim e correção dos itens que responderam sim à primeira pergunta. Se esse número passa de uma semana, a primeira pergunta não está sendo feita.
- Janela aberta em item de catálogo de exploração. Quantos dias cada falha em exploração conhecida ficou sem correção no seu ambiente, caso a caso. Um item por mês, no máximo quatro. É o indicador que cabe inteiro em um slide.

O recorte local, que é leitura nossa

Duas coisas mudam esse cálculo no Brasil. A primeira é parque de Office em versão perpétua, comum em órgão público e em empresa de médio porte, onde a atualização do Outlook não chega por canal automático e depende de pacote distribuído. Para esses, a medida de rede não é complemento, é a correção efetiva nas próximas semanas.

A segunda é a janela de manutenção de servidor de borda. Exchange local ainda roda em muita operação, e a mesma equipe que cuida dele cuida de dez outras coisas. Quando o boletim tem mil itens, a tentação é esperar o pacote cumulativo do mês seguinte. Esse é o mês em que isso custa caro, porque seis dos itens que importam estão em serviço que atende pedido de quem não tem conta.

O que ninguém publicou, e que convém não preencher com suposição: quem explorou a falha do Outlook, contra quem, e por quanto tempo antes da correção. A Microsoft não disse. Enquanto não disser, a hipótese de trabalho razoável é que captura de hash por mensagem preparada é barata e já estava em uso em campanha comum, não só em operação direcionada.

Quatro decisões que cabem nesta semana

01 · decisão

Escolher qual contagem a organização vai usar, e usar só ela

Fixar o critério, com ou sem as CVEs de terceiros que chegam pelo canal do navegador, e manter o mesmo número no painel e no relatório. Indicador que troca de denominador todo mês não serve para comparar meses.

02 · decisão

Separar a fila de borda da fila de estação, com responsáveis diferentes

Os seis itens de execução remota em serviço de identidade e de borda não competem por recurso com as centenas de elevações locais. Hoje elas competem, porque entram na mesma lista ordenada por nota.

03 · decisão

Aplicar as medidas de NTLM independentemente do patch do Outlook

Bloqueio de SMB e NTLM saindo para a internet, auditoria antes de restrição, usuários protegidos e assinatura de SMB. Quatro mudanças de configuração que sobrevivem a este boletim e ao próximo.

04 · decisão

Registrar a janela aberta em item de exploração conhecida, caso a caso

Um único indicador, com data de publicação, data de correção e justificativa de qualquer atraso. É o que um auditor pede e é o que um incidente vai cobrar depois.

Fontes

- Tenable · Microsoft's November 2026 Patch Tuesday Addresses 1,093 CVEs (CVE-2026-124194), com a contagem por severidade, a distribuição por tipo e os dez produtos com mais CVEs. `https://www.tenable.com/blog/microsoft-november-2026-patch-tuesday-addresses-1093-cves-cve-2026-124194`
- SANS Internet Storm Center · Microsoft Patch Tuesday November 2026, com o total incluindo as CVEs do Chromium e a leitura de Johannes Ullrich. `https://isc.sans.edu/diary/33508`
- Microsoft · CVE-2026-124194, Microsoft Outlook Spoofing Vulnerability, aviso do fabricante com a severidade, o vetor e o crédito de descoberta. `https://msrc.microsoft.com/update-guide/advisory/CVE-2026-124194`
- Dark Reading · November Patch Tuesday: An Overflowing Cornucopia of CVEs, cobertura do boletim e das recomendações de triagem. `https://www.darkreading.com/vulnerabilities-threats/november-patch-tuesday-cornucopia-cves`