Mais de 28.000 servidores Microsoft Exchange expostos online à vulnerab

Data: 2025-08-09 10:28:27

Autor: Inteligência Against Invaders

A comunidade de segurança cibernética enfrenta uma ameaça significativa, pois a verificação de dados revela que mais de 28.000 servidores Microsoft Exchange não corrigidos permanecem expostos na Internet pública, vulneráveis a uma falha crítica de segurança designada CVE-2025-53786.

Essa vulnerabilidade de alta gravidade, que carrega uma pontuação CVSS de 8,0 em 10, permite que invasores com acesso administrativo a servidores Exchange locais escalem privilégios em ambientes de nuvem conectados do Microsoft 365 sem deixar trilhas de auditoria facilmente detectáveis.

A descoberta levou à intervenção imediata do governo e a pedidos urgentes para que organizações em todo o mundo implementem medidas de segurança de emergência.

Exposição global maciça ameaça a segurança

A vulnerabilidade afeta as implantações híbridas do Microsoft Exchange Server, com dados de varredura da The Shadowserver Foundation identificando os Estados Unidos, Alemanha e Rússia como os três principais países que abrigam as maiores concentrações de servidores vulneráveis expostos.

A falha, rastreada como CVE-2025-53786, foi oficialmente documentada pela Microsoft em 6 de agosto de 2025, seguindo técnicas de exploração detalhadas demonstradas pelo pesquisador de segurança Dirk-Jan Mollema da Outsider Security na conferência de segurança cibernética Black Hat.

A vulnerabilidade decorre da arquitetura de implantação híbrida do Exchange da Microsoft, que tradicionalmente usava uma entidade de serviço compartilhada entre servidores Exchange locais e Exchange Online para autenticação.

Essa configuração cria um caminho perigoso para Escalonamento de privilégios ataques, pois os invasores que comprometem sistemas locais podem estender seu acesso a ambientes de nuvem.

A Agência de Segurança Cibernética e Infraestrutura (CISA) avaliou isso como uma vulnerabilidade de alta gravidade com implicações significativas para a segurança corporativa.

A CISA respondeu rapidamente a essa ameaça, emitindo a Diretiva de Emergência 25-02 em 7 de agosto, obrigando as agências federais a resolver a vulnerabilidade até as 9:00 ET na segunda-feira, 11 de agosto.

O diretor interino da CISA, Madhu Gottumukkala, enfatizou a natureza crítica da situação, afirmando que a agência está “tomando medidas urgentes para mitigar essa vulnerabilidade que representa um risco significativo e inaceitável para os sistemas federais dos quais os americanos dependem”.

A diretiva de emergência reflete a gravidade do impacto potencial, pois a exploração bem-sucedida pode permitir que os invasores aumentem os privilégios “dentro do ambiente de nuvem conectado da organização sem deixar rastros facilmente detectáveis e auditáveis”.

A Microsoft e a CISA alertam sobre “riscos significativos e inaceitáveis” para organizações que operam configurações híbridas do Exchange que não implementaram as diretrizes de segurança de abril de 2025.

Estratégias de Exploração e Mitigação

A vulnerabilidade explora tokens de acesso especiais usados para comunicação do servidor Exchange com Microsoft 365, que não pode ser cancelado depois de roubado, fornecendo aos invasores até 24 horas de acesso não verificado.

Como Mollema explicou durante sua apresentação do Black Hat, “Esses tokens são basicamente válidos por 24 horas.

Você não pode revogá-los. Então, se alguém tem esse token, não há absolutamente nada que você possa fazer do ponto de vista defensivo”.

As organizações devem tomar medidas imediatas para proteger seus sistemas por meio das seguintes etapas críticas:

- **Instale as atualizações de hotfix do Exchange Server de abril de 2025 da Microsoft** para corrigir a vulnerabilidade subjacente.
- **Implantar aplicativos híbridos dedicados do Exchange** para substituir as configurações da entidade de serviço compartilhado.
- **Limpar credenciais de entidade de serviço herdadas** que poderiam fornecer caminhos de acesso não autorizados.
- **Implementar alterações de configuração** em ambientes híbridos do Exchange Server, conforme descrito nas diretrizes de segurança da Microsoft.
- **Examinar e atualizar políticas de acesso condicional** para fortalecer os controles de autenticação.

A Microsoft já havia começado a resolver essa vulnerabilidade por meio de alterações de segurança anunciadas em 18 de abril de 2025, introduzindo uma transição de entidades de serviço compartilhadas para aplicativos híbridos dedicados do Exchange.

A Microsoft planeja bloquear permanentemente o tráfego dos Serviços Web do Exchange usando a entidade de serviço compartilhada após 31 de outubro de 2025, como parte de sua transição para uma arquitetura mais segura da API do Graph.