Os hackers exploraram a falha do Zimbra como dia zero usando arquivos

Data: 2025-10-05 22:11:11

Autor: Inteligência Against Invaders

Pesquisadores monitorando para maiores. Anexos do calendário ICSdescobriu que uma falha no

Zimbra Collaboration Suite (ZCS) foi usada em ataques de dia zero no início do ano.

Os arquivos ICS, também conhecidos como arquivos iCalendar, são usados para armazenar informações de calendário e agendamento (reuniões, eventos e tarefas) em texto simples e para trocá-las entre vários aplicativos de calendário.

Os agentes de ameaças exploraram o CVE-2025-27915, uma vulnerabilidade de cross-site scripting (XSS) no ZCS 9.0, 10.0 e 10.1, para fornecer uma carga útil JavaScript aos sistemas de destino.

A vulnerabilidade decorre da limpeza insuficiente do conteúdo HTML em arquivos ICS, o que permitiu que invasores executassem JavaScript arbitrário na sessão da vítima, como definir filtros que redirecionam mensagens para eles.

Zimbra Resolveu o problema de segurança em 27 de janeiroao lançar ZCS 9.0.0 P44, 10.0.13 e 10.1.5, mas não mencionou nenhuma atividade de exploração ativa.

No entanto, pesquisadores da StrikeReady, uma empresa que desenvolve uma plataforma de gerenciamento de ameaças e operações de segurança orientada por IA, descobriram o ataque depois de ficarem de olho no . Arquivos ICS maiores que 10 KB e incluídos código JavaScript.

Eles determinaram que os ataques começaram no início de janeiro, antes de Zimbra lançar o patch.

O agente da ameaça falsificou o Escritório de Protocolo da Marinha da Líbia em um e-mail que entregou uma exploração de dia zero que teve como alvo uma organização militar brasileira.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]pesquisadores", a carga útil é projetada para roubar dados do Zimbra Webmail, como credenciais, e-mails, contatos e pastas compartilhadas.

StrikeReady diz que o código malicioso é implementado para ser executado no modo assíncrono e em váriasExpressões de Função Imediatamente Invocadas (IIFEs). Os pesquisadores descobriram que ele pode realizar as seguintes ações:

- Criarcampos de nome de usuário/senha ocultos
- Roubar credenciais de formulários de login
- Monitore a atividade do usuário (mouse e teclado) e faça logout de usuários inativos para

acionar o roubo
- UseZimbra SOAP API para pesquisar pastas e recuperar e-mails
- Enviar conteúdo de e-mail para o invasor (repete a cada 4 horas)
- Filtro Adda chamado “Correo” para encaminhar e-mails para um endereço Proton
- Colete esses artefatos de autenticação/backup e exfiltre-os
- Exfiltrarcontatos, listas de distribuição e pastas compartilhadas
- Adda Atraso de 60 segundos antes da execução
- Enforcea porta de execução de 3 dias (só é executada novamente se ?3 dias desde a última execução)
- Ocultar elementos da interface do usuário (UI) para reduzir pistas visuais

O StrikeReady não pôde atribuir esse ataque com alta confiança a nenhum grupo de ameaças conhecido, mas observou que há um pequeno número de invasores que podem descobrir vulnerabilidades de dia zero em produtos amplamente usados, mencionando que um “grupo vinculado à Rússia é especialmente prolífico”.

Os pesquisadores também mencionaram que táticas, técnicas e procedimentos semelhantes (TTPs) foram observados em ataques atribuídos a UNC1151 – um grupo de ameaça que Mandiant ligado ao governo bielorrusso.

O relatório da StrikeReady compartilha Indicadores de comprometimento e uma versão desofuscada do código JavaScript do ataque leveragin . INC arquivos de calendário.

O BleepingComputer entrou em contato com o Zimbra com perguntas sobre essa atividade e atualizaremos este post com sua declaração assim que a recebermos.