Hackers exploraram falha do Zimbra como dia zero usando arquivos iCale

Data: 2025-10-05 15:15:33

Autor: Inteligência Against Invaders

Pesquisadores monitorando para maiores. Os anexos do calendário ICS descobriram que uma falha no Zimbra Collaboration Suite (ZCS) foi usada em ***dia zero*** ataques no início do ano. Os arquivos ICS, ou arquivos iCalendar, armazenam informações de calendário em texto simples, como reuniões e eventos, e permitem a troca entre diferentes 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 existe devido à limpeza inadequada do conteúdo HTML em arquivos ICS, permitindo que invasores executem JavaScript prejudicial na sessão da vítima e redirecionem mensagens.

A Zimbra abordou o problema de segurança em 27 de janeiro lançando ZCS 9.0.0 P44, 10.0.13 e 10.1.5, mas não mencionou nenhuma atividade de exploração ativa. Pesquisadores da StrikeReady, uma empresa especializada em segurança orientada por IA e gerenciamento de ameaças, identificaram o ataque monitorando . Arquivos ICS com mais de 10 KB que continham código JavaScript.

Eles determinaram que os ataques começaram no início de janeiro, antes de Zimbra lançar o patch. Um hacker fingiu ser o Escritório de Protocolo da Marinha da Líbia em um e-mail que continha um exploit de dia zero direcionado a uma organização militar brasileira.

O e-mail malicioso incluía um pequeno arquivo ICS com um arquivo JavaScript oculto.

A análise mostra que a carga útil é médiat para roubar dados do Zimbra Webmail, como detalhes de login, e-mails, contatos e pastas compartilhadas.

O StrikeReady relata que o código mal-intencionado é executado de forma assíncrona e usa IIFEs (Expressões de Função Invocadas Imediatamente). Os pesquisadores identificaram suas capacidades, incluindo:

Criar campos de nome de usuário/senha ocultos
Roubar credenciais de formulários de login
Monitore a atividade do usuário (mouse e teclado) e desconecte usuários inativos para acionar o roubo
Use a API SOAP do Zimbra para pesquisar pastas e recuperar e-mails
Enviar conteúdo de e-mail para o invasor (repete a cada 4 horas)
Adicione um filtro chamado “Correo” para encaminhar e-mails para um endereço Proton
Colete esses artefatos de autenticação/backup e exfiltre-os
Exfiltrar contatos, listas de distribuição e pastas compartilhadas
Adicione um atraso de 60 segundos antes da execução

Impor um portão de execução de 3 dias (só é executado novamente se ?3 dias desde a última execução)
Ocultar elementos da interface do usuário 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 ligado à Rússia é especialmente prolífico”.

Os pesquisadores observaram que táticas, técnicas e procedimentos semelhantes (TTPs) são vistos em ataques ligados ao UNC1151, um grupo de ameaças associado ao governo bielorrusso pela Mandiant.

O relatório da StrikeReady compartilha indicadores de comprometimento e uma versão desofuscada do código JavaScript do ataque leveragin . INC arquivos de calendário. BleepingComputador ***reportado*** que eles não receberam nenhuma resposta ao publicar o relatório de Zimbra.