Usuários do Zimbra são alvo de exploração de dia zero usando anexos do

Data: 2025-10-06 08:08:55

Autor: Inteligência Against Invaders

Usuários do Zimbra são alvo de exploração de dia zero usando anexos do iCalendar

Os agentes de ameaças exploraram um dia zero do Zimbra por meio do iCalendar malicioso (. ICS) usados para entregar ataques por meio de anexos de calendário.

Os pesquisadores do StrikeReady descobriram que os agentes de ameaças exploraram a vulnerabilidade CVE-2025-27915 no Zimbra Collaboration Suite em ataques de dia zero usando o iCalendar malicioso (. ICS). Esses arquivos, usados para compartilhar dados de calendário, foram armados para fornecer cargas úteis de JavaScript aos sistemas visados no início deste ano.

CVE-2025-27915 é uma falha de XSS armazenada no Zimbra Collaboration Suite (versões 9.0–10.1) causada por limpeza inadequada de HTML em arquivos ICS. Quando as vítimas abrem um e-mail com uma entrada ICS maliciosa, o JavaScript é executado por meio de um , permitindo que invasores sequestrem sessões, definam redirecionamentos de e-mail e exfiltrem dados.

*“No início de 2025, um aparente remetente de193.29.58.37falsificou o Escritório de Protocolo da Marinha da Líbia para enviar um exploit de dia zero no Collaboration Suite do Zimbra,*CVE-2025-27915*, visando as forças armadas do Brasil. Isso alavancou um arquivo malicioso . ICS, um arquivo popular*formato de calendário*.” lê o* relatório *publicado pela StrikeReady.*

Os pesquisadores descobriram os ataques enquanto analisavam arquivos ICS maiores que 10 KB que continham JavaScript ofuscado incorporado.

O script malicioso tem como alvo o Zimbra Webmail, roubando credenciais, e-mails, contatos e pastas compartilhadas. Ele exfiltra dados para ffrk.net e usa várias técnicas de evasão; o código malicioso atrasa sua execução em 60 segundos, limita a atividade a três dias, oculta pistas de interface do usuário e desconecta usuários inativos para roubar dados. Os pesquisadores também descobriram que o script é executado de forma assíncrona usando várias funções de Expressões de Função Invocada (IIFEs).

Abaixo estão as funções suportadas pelo malware:

- Injeta campos de formulário ocultos para capturar nomes de usuário e senhas sem indicadores de interface do usuário visíveis.
- Exfiltra credenciais inseridas em formulários de autenticação.
- Rastreia a atividade de entrada (mouse/teclado) e, se o usuário ficar ocioso, encerra a sessão para habilitar o roubo de dados.

- Consulta a API SOAP do Zimbra para enumerar pastas e receber mensagens de e-mail.
- Periodicamente (a cada ~4 horas) carrega o conteúdo de e-mail capturado no servidor do invasor.
- Instala uma regra de encaminhamento de e-mail intitulada “Correo” que redireciona mensagens para um endereço ProtonMail.
- Reúne artefatos de autenticação e tokens de backup e os envia ao invasor.
- Extrai catálogos de endereços, listas de distribuição e itens de pastas compartilhadas.
- Atrasa sua carga útil em 60 segundos após a injeção para evitar a detecção rápida.
- Restringe a atividade total a uma janela operacional de três dias antes de exigir um período de resfriamento.
- Obscurece ou remove elementos de interface para minimizar sinais visuais de comprometimento.
- Opera de forma assíncrona em vários blocos de código independentes para fragmentar a execução e complicar a análise.

O StrikeReady não conseguiu atribuir o ataque a um grupo específico, mas apontou que apenas alguns atores com bons recursos têm a capacidade de realizar ataques de dia zero. Os pesquisadores observaram TTPs semelhantes aos vinculados ao grupo APT bielorrusso UNC1151.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Zimbra zero-day)