AVISO DE SEGURANÇA — EXPLORAÇÃO ATIVA

RCE não autenticado em servidores Zimbra via injeção de log no SNMP/Swatchdog — CVE-2026-73570

Uma falha de sanitização no monitor de log do Zimbra Collaboration Suite permite execução remota de comandos sem autenticação, apenas enviando um e-mail. A campanha está sendo explorada em massa e já resultou em backdoors fileless, mineração de criptomoeda, webshells e roubo de credenciais em ambientes reais.

CRÍTICA · pré-autenticação, sem interação do usuário

Afeta versões legadas do Zimbra (linhas anteriores à 10.1.20)

Exploração em massa confirmada · scanners automatizados ativos

01 O que é a vulnerabilidade

O Zimbra inclui um daemon de monitoramento (Swatchdog) que lê continuamente os logs do Postfix procurando por um padrão de texto específico para disparar ações automáticas. O problema: o conteúdo que aparece nesse log pode ser controlado por qualquer pessoa que envie um e-mail para o servidor — e o Swatchdog não sanitiza esse conteúdo antes de repassá-lo a um shell.

Resultado: um remetente externo, sem nenhuma credencial, consegue injetar comandos de sistema que são executados com os privilégios do usuário de serviço do Zimbra. Nenhum clique, anexo ou login é necessário — o gatilho é uma mensagem SMTP.

02 Como a exploração funciona, passo a passo

1. O atacante envia um e-mail (via `MAIL FROM` / `RCPT TO`) contendo o texto exato que o Swatchdog está configurado para vigiar, com um comando de shell embutido usando substituição de variável `$(...)`.
2. O Postfix recusa a mensagem por sintaxe inválida — mas isso não importa: ele registra a tentativa no log antes de rejeitar.
3. O Swatchdog lê essa linha de log, reconhece o padrão monitorado e dispara sua ação configurada, tratando o conteúdo injetado como parte de um comando de shell legítimo.
4. O comando é executado com os privilégios do processo do Zimbra. A partir daqui, o corpo do e-mail é o payload — o atacante decide o que roda.

Pré-requisito para exploração: o componente SNMP do Zimbra e o daemon Swatchdog precisam estar ativos no host. Em ambientes onde esse serviço foi habilitado por engano ou por herança de configuração antiga, a janela de exposição pode durar semanas antes de ser notada.

03 O que atacantes reais estão fazendo depois de entrar

Múltiplos grupos independentes, com níveis de sofisticação distintos, já usam essa falha ativamente. Os payloads observados se agrupam em quatro famílias de comportamento:

FILELESS

Backdoor em memória com C2

Binário executado direto na RAM (sem tocar disco), mascarado como processo legítimo do sistema, com beacon periódico para infraestrutura de CDN usada como fachada de C2.

CRYPTOJACKING

Minerador via persistência em cron

Script auto-replicante que mascara o nome do processo, mata mineradores concorrentes e recria sua própria entrada de cron a cada poucos segundos para resistir à limpeza manual.

VARREDURA EM MASSA

Webshells automatizadas

Ferramentas públicas de exploração plantam shells JSP genéricas em diretórios públicos do painel web, com nomes que imitam arquivos legítimos do sistema.

OPERAÇÃO MANUAL

Exfiltração e limpeza de rivais

Ator mais avançado: entrega em múltiplos estágios, forjamento de timestamp do arquivo malicioso, extração do arquivo de configuração com credenciais, remoção de shells de outros grupos e fechamento do próprio vetor de entrada.

04 Por que isso importa

- Execução remota de comandos sem qualquer autenticação — o vetor é só um e-mail.
- Arquivo de configuração local do Zimbra contém credenciais de LDAP, banco de dados e conta administrativa — se lido pelo atacante, deve ser tratado como totalmente comprometido.
- Técnica fileless (execução em memória) evita detecção por antivírus tradicional e verificação de integridade de arquivos.
- Vários grupos podem estar explorando o mesmo host ao mesmo tempo, competindo por persistência e recursos.
- Um ator mais sofisticado pode identificar e remover as evidências de outros — mascarando a real linha do tempo do incidente.
- Ambientes vulneráveis podem estar comprometidos há semanas antes de qualquer sintoma visível (CPU, memória) aparecer.

05 Mitigação recomendada

- [ ] Atualizar para uma versão do Zimbra corrigida contra CVE-2026-73570 (Zimbra 10.1.20 ou superior).
- [ ] Rotacionar credenciais de LDAP, banco de dados e conta admin se houver qualquer suspeita de leitura do arquivo de configuração local.
- [ ] Implementar monitoramento de integridade de arquivos nos diretórios públicos da aplicação web para detectar novas webshells.
- [ ] Se o upgrade não for imediato, desabilitar o daemon Swatchdog como mitigação temporária — ele é pré-requisito direto do vetor.
- [ ] Monitorar processos com nomes de serviços do sistema (ex. daemons de tempo/rede) rodando sob o usuário de serviço do Zimbra — sinal clássico de mascaramento.
- [ ] Auditar chaves SSH, contas e permissões administrativas do host — presuma janela de acesso não detectada até prova em contrário.

Report gerado por felipeold com apoio de hiratakun — Comunidade Hackers Hive Discord

compartilhado na **Hackers Hive** — Discord