Libraesva ESG emite correção emergencial para bug explorado por hacker

Data: 2025-09-23 20:30:14

Autor: Inteligência Against Invaders

A Libraesva lançou uma atualização de emergência para sua solução Email Security Gateway (ESG)

para corrigir uma vulnerabilidade explorada por agentes de ameaças que se acredita serem

patrocinados pelo Estado.

O produto de segurança de e-mail protege os sistemas de e-mail contra phishing, malware, spam, comprometimento de e-mail comercial e falsificação, usando uma arquitetura de proteção multicamadas.

De acordo com o fornecedor, o Libraesva ESG é usado por milhares de pequenas e médias empresas, bem como grandes empresas em todo o mundo, atendendo mais de 200.000 usuários.

O problema de segurança, rastreado em CVE-2025-59689, receberam escore de gravidade média. Ele é acionado pelo envio de um anexo de e-mail criado com códigos maliciosos e permite a execução de comandos shell arbitrários de uma conta de usuário sem privilégios.

“O Libraesva ESG é afetado por uma falha de injeção de comando que pode ser acionada por um e-mail malicioso contendo um anexo compactado especialmente criado, permitindo a execução potencial de comandos arbitrários como um usuário sem privilégios”, diz o Boletim de segurança.

“Isso ocorre devido a uma higienização inadequada durante a remoção do código ativo dos arquivos contidos em alguns formatos de arquivo compactados”, explica Libraesva.

De acordo com o fornecedor, houve pelo menos um incidente confirmado de um invasor “que se acredita ser uma entidade estatal hostil estrangeira” aproveitando a falha nos ataques.

CVE-2025-59689 afeta todas as versões do Libraesva ESG a partir de 4.5 e posteriores, mas as correções estão disponíveis no seguinte:

- 5.0.31
- 5.1.20
- 5.2.31
- 5.3.16
- 5.4.8
- 5.5.7

Os clientes que usam versões abaixo da 5.0 devem atualizar manualmente para uma versão compatível, pois atingiram o fim da vida útil e não receberão um patch para CVE-2025-59689.

Libraesva diz que o patch foi lançado como uma atualização de emergência 17 horas após a

descoberta da exploração. A correção foi implantada automaticamente em implantações na nuvem e no local.

O patch inclui uma correção de sanitização para resolver a causa raiz da falha, uma verificação automatizada de indicadores de comprometimento para determinar se o ambiente já foi violado e um módulo de autoavaliação que verifica a aplicação correta da atualização de segurança.

O fornecedor também comentou sobre o ataque, dizendo que o agente da ameaça com foco em um único dispositivo indica precisão, destacando a importância de uma ação rápida de correção.

[IMAGEM REMOVIDA]