



BOLETIM DE SEGURANÇA

**Vulnerabilidades críticas no Cacti facilitam a execução
de códigos maliciosos**



Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research](#)



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall](#)



ISH —

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH —

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH —

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	5
2	Detalhes sobre as vulnerabilidades.....	6
3	Recomendações.....	7
4	Referências	8
5	Autores.....	9

LISTA DE FIGURAS

Figura 1 – Execução de código PHP arbitrário. 6

1 SUMÁRIO EXECUTIVO

Os responsáveis pela plataforma de monitoramento de redes e gestão de incidentes Cacti, corrigiram recentemente doze vulnerabilidades de segurança. Entre elas, destacam-se duas falhas críticas que, se exploradas, poderiam permitir a execução de códigos arbitrários por parte de invasores. Essas correções são um passo importante para fortalecer a segurança do sistema contra possíveis ataques mal-intencionados.

2 DETALHES SOBRE AS VULNERABILIDADES

A vulnerabilidade [CVE-2024-25641](#) é uma falha que permite usuários com direitos de "Importar modelos" no sistema Cacti explorem a funcionalidade de "Importação de pacote" para realizar escrita de arquivos à vontade, o que pode levar à execução de código PHP arbitrário no servidor.

A vulnerabilidade [CVE-2024-29895](#) é uma falha que possibilita a execução de comandos no servidor por usuários não autenticados, aproveitando-se da configuração "register_argc_argv" do PHP, caso esteja habilitada, resultando em um controle total do servidor por parte do atacante.

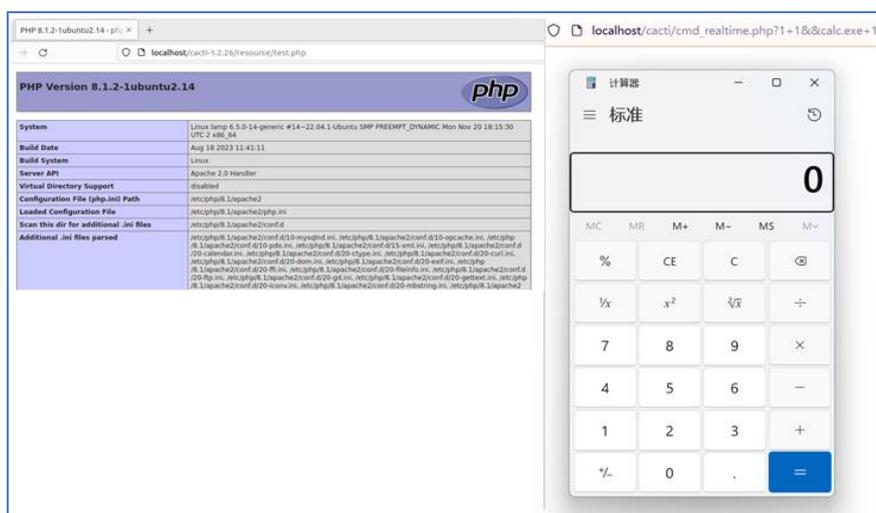


Figura 1 – Execução de código PHP arbitrário.

O Cacti também está informou outras duas vulnerabilidades e ambas com criticidade alta, em que permitem a execução de código não autorizado. Uma delas é a injeção de SQL [CVE-2024-31445](#), na "api_automation.php" que permite que usuários autenticados realizem escalonamento de privilégios e execução remota de código. A vulnerabilidade [CVE-2024-31459](#), se refere a um bug de inclusão de arquivo no "lib/plugin.php" que pode ser combinado com vulnerabilidades de injeção de SQL para resultar na execução remota de código.

10 das 12 vulnerabilidades, com exceção de [CVE-2024-29895](#) e [CVE-2024-30268](#), impactam todas as versões do Cacti, incluindo e anteriores a 1.2.26. Elas foram corrigidas na versão 1.2.27 lançada em maio de 2024. As outras duas falhas afetam as versões de desenvolvimento 1.3.x. Essas correções surgem após a descoberta, oito meses após a divulgação de outra vulnerabilidade [CVE-2023-39361](#) classificada como crítica de injeção de SQL que poderia permitir que um invasor obtivesse permissões elevadas e executasse código malicioso. No início de 2023, uma terceira vulnerabilidade [CVE-2022-46169](#) classificada como crítica ficou sob exploração ativa, permitindo que agentes de ameaças violassem servidores Cacti expostos à Internet para entregar malware de botnet, como MooBot e ShellBot.

3 RECOMENDAÇÕES

De acordo com a Cacti, as vulnerabilidades foram todas corrigidas e recomenda-se que os usuários [atualizem](#) para versão 1.2.27 lançada em 13 de maio de 2024.

4 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Cacti](#)
- [Thehackernews](#)
- [NVD](#)

5 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH