BOLETIM DE SEGURANÇA

Falha crítica no plug-in WP-Automatic do WordPress, sendo explorada em ataques

heimdall
security research
A DIVISION OF ISH

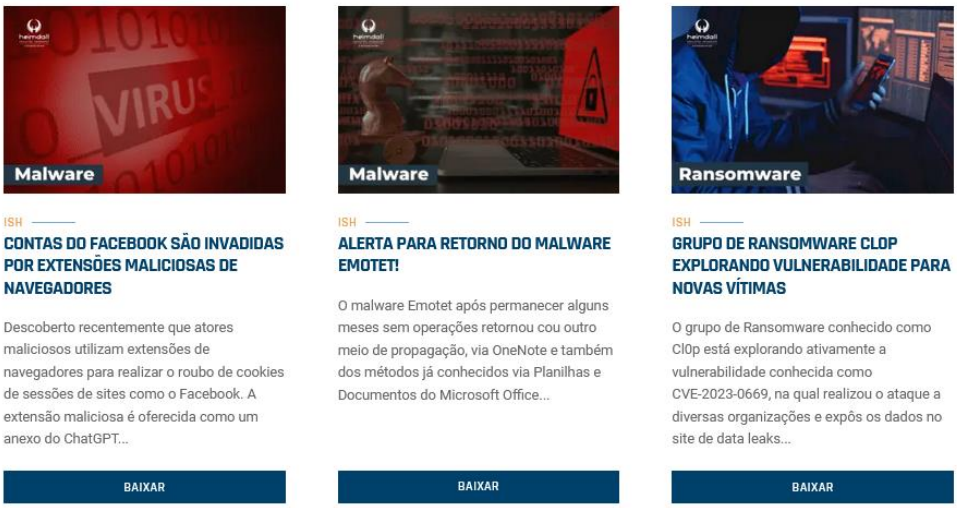
TLP: CLEAR

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



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A vulnerabilidade crítica CVE-2024-27956 no plugin WP Automatic para WordPress está sendo explorada por agentes mal-intencionados para criar contas administrativas e instalar backdoors, garantindo acesso prolongado ao site. O plugin, presente em mais de 30.000 sites, facilita a automação da importação e publicação de conteúdo de diversas fontes online.

Figura 1 – Detalhes sobre a vulnerabilidade.

2 DETALHES DA VULNERABILIDADE E EXPLORAÇÕES

A vulnerabilidade CVE-2024-27956 afeta o plugin WP Automatic do WordPress, sendo uma falha de injeção SQL que permite ataques não autenticados. Ela foi identificada com uma pontuação crítica de 9,9 no sistema CVSS e afeta todas as versões do plugin até a 3.92.0. Esta vulnerabilidade permite que atacantes executem comandos SQL arbitrários no banco de dados de um site, possibilitando a criação de contas de administrador, o upload de arquivos maliciosos e até a tomada total do controle do site.

Os ataques exploram especificamente a função de autenticação do usuário do plugin, permitindo que os atacantes insiram consultas SQL maliciosas para manipular o banco de dados do site. Desde a divulgação dessa vulnerabilidade, foram registrados milhões de tentativas de ataque, culminando em tentativas de criar acessos administrativos persistentes através de backdoors e scripts maliciosos.

Cadeia dos ataques observados nas explorações

1. **Injeção de SQL (SQLi)**: Os invasores aproveitam a vulnerabilidade do SQLi no plug-in WP-Automatic para executar consultas não autorizadas ao banco de dados.
2. **Criação de usuário administrador**: com a capacidade de executar consultas SQL arbitrárias, os invasores podem criar novas contas de usuário de nível administrativo no WordPress.
3. **Upload de malware**: depois que uma conta de administrador é criada, os invasores podem fazer upload de arquivos maliciosos, normalmente web shells ou backdoors, para o servidor do site comprometido.
4. **Renomeação de arquivo**: o invasor pode renomear o arquivo WP-Automatic vulnerável, para garantir que somente ele possa explorá-lo.

Uma vez que um site WordPress é invadido, os atores maliciosos asseguram acesso duradouro através da criação de backdoors e camuflagem do código. Para permanecerem não detectados e manter o controle, eles podem renomear o arquivo vulnerável do WP-Automatic, o que complica a identificação e o bloqueio do problema por parte dos proprietários dos sites ou de ferramentas de segurança. Isso também pode servir como uma estratégia para impedir que outros criminosos explorem os mesmos sites comprometidos. Ademais, utilizando os privilégios elevados que adquirem, os invasores frequentemente instalam plugins e temas que permitem o upload de arquivos e a edição de código, uma prática comum em sites comprometidos para facilitar a manipulação contínua do site.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo, poderão ser adotadas medidas visando a mitigação e identificação da referida *ameaça*, como por exemplo:

Mantenha os plug-ins atualizados

- Certifique-se de que todos os plug-ins do WordPress, incluindo o Automatic, estejam atualizados regularmente para as versões mais recentes para corrigir vulnerabilidades conhecidas. Para a correção da vulnerabilidade citada neste relatório, o plugin WP-Automatic deve estar na versão **3.92.1**

Implemente um Web Application Firewall (WAF)

- O WAF desempenha um papel crucial na detecção e mitigação de ataques de injeção de SQL. Eles analisam solicitações HTTP em tempo real, procurando padrões e assinaturas suspeitas comumente associadas ao SQL tentativas de injeção. Ao monitorar o comportamento de aplicações web, o WAF pode identificar atividades anormais indicativas de um ataque.

Backup regular

- Estabeleça um cronograma de backup regular para garantir que seu site os dados são copiados de forma consistente. Dependendo da frequência das atualizações e alterações em seu site, backups diários ou semanais podem ser apropriados.

Identifique usuários não autorizados

- Verifique se há algum usuário não autorizado ou suspeito contas que possam ter sido criadas sem a devida autorização. Procurar contas com privilégios administrativos que não pertencem a usuários legítimos ou contas com padrões de atividade incomuns. Desative ou remova contas de usuário que estejam não são mais necessários ou estão inativos.

4 INDICADORES DE COMPROMISSOS

Conforme a WPScan, se você encontrar algum dos seguintes indicadores abaixo, significa que seu site foi comprometido por esta campanha ativa:

- Usuário administrador com nome começando com **xtw**.
- O arquivo vulnerável *"/wp-content/plugins/wp-automatic/inc/csv.php"* renomeado para algo como *"/wp-content/plugins/wp-automatic/inc/csv65f82ab408b3.php"*
- Os seguintes arquivos com hash SHA-1 foram descartados no sistema de arquivos do seu site:

b0ca85463fe805ffdf809206771719dc571eb052 *web.php*

8e83c42ffd3c5a88b2b2853ff931164ebce1c0f3 *index.php*

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **WPScan**
- **Patchstack**
- **NVD**

heimdall
security research
A DIVISION OF ISH