BOLETIM DE SEGURANÇA

Falha crítica no Plugin Forminator do WordPress afetando milhares de sites

heimdall
security research
A DIVISION OF ISH

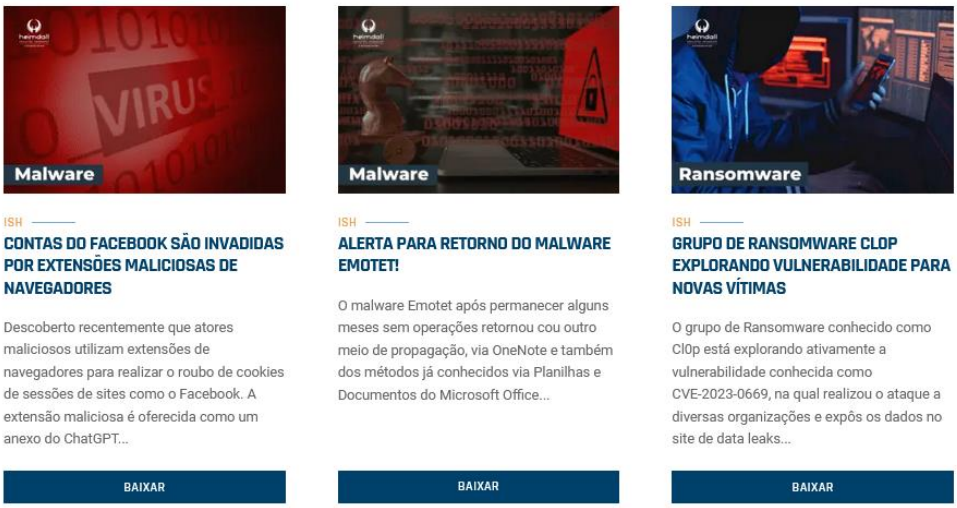
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Recentemente o CERT do Japão publicou um alerta em seu portal de notas de vulnerabilidade (JVN) alertando sobre a existência de uma falha de gravidade crítica (**CVE-2024-28890**, **CVSS v3: 9.8**) no plugin Forminator do WordPress, utilizado em centenas de milhares de sites, pode permitir que um invasor remoto carregue malware em sites usando o plugin. Fora esta vulnerabilidade, o alerta também referência mais duas no plugin.

2 DETALHES DAS VULNERABILIDADES

O boletim de segurança do JPCERT lista as três vulnerabilidades a seguir:

CVE-2024-28890

- Validação insuficiente de arquivos durante o upload de arquivos, permitindo que um invasor remoto carregue e execute arquivos maliciosos no servidor do site. Impacta o Forminator 1.29.0 e versões anteriores.

CVE-2024-31077

- Falha de injeção de SQL que permite que invasores remotos com privilégios de administrador executem consultas SQL arbitrárias no banco de dados do site. Impacta o Forminator 1.29.2 e anteriores.

CVE-2024-31857

- Falha de script entre sites (XSS) que permite que um invasor remoto execute HTML arbitrário e código de script no navegador de um usuário se for enganado a seguir um link especialmente criado. Impacta o Forminator 1.15.4 e versões anteriores.

Apesar da gravidade dos problemas com o plugin Forminator, detalhes técnicos específicos sobre como as vulnerabilidades podem ser exploradas não foram divulgados publicamente até as atualizações mais recentes.

3 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Atualização do plugin Forminator para a versão 1.29.3 o mais rápido possível, que corrige todas as três falhas.

Use apenas plugins confiáveis

- Instale plugins apenas de fontes confiáveis, como o diretório oficial de plugins do WordPress. Verifique as avaliações e o número de instalações ativas, além da frequência das atualizações do plugin.

Limite o número de plugins

- Quanto mais plugins você instalar, maior o risco de segurança. Use apenas os plugins essenciais e desinstale os que não estão sendo usados.

Faça backups regulares

- Antes de atualizar um plugin, faça um backup completo do site. Isso permite que você restaure o site para uma versão anterior caso algo dê errado.

Verifique as permissões

- Certifique-se de que os plugins não concedam permissões administrativas desnecessárias aos usuários. Isso pode expor seu site a riscos de segurança se essas permissões caírem nas mãos erradas.

Use um plugin de segurança

- Instale um plugin de segurança de qualidade para monitorar e proteger seu site contra ataques comuns, como tentativas de força bruta e injeção de SQL.

Revise o código dos plugins

- Se possível, revise o código dos plugins para verificar práticas de codificação seguras. Plugins com códigos mal escritos podem abrir brechas de segurança.

Implemente autenticação de dois fatores (2FA)

- Adicione uma camada extra de segurança ao processo de login, exigindo uma segunda forma de verificação além da senha.

Configure o HTTPS

- Use um certificado SSL para criptografar a comunicação entre o navegador do usuário e o seu servidor, protegendo os dados transmitidos.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **JPCERT**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH