TLP: CLEAR

PESQUISA DE WEB Exploitation

Execução Remota de Código no WordPress através do Plugin WPBookit (CVE-2025-6058)

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1. INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência Heimdall da ISH Tecnologia, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: Estratégico, Tático e Operacional, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2. ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

O ecossistema *WordPress* é amplamente adotado por *sites* institucionais, *e-commerces* e plataformas de conteúdo, o que o torna um alvo recorrente de campanhas maliciosas. Nesse contexto, a vulnerabilidade **CVE-2025-6058** representa um risco crítico para aplicações que utilizam o plugin ***WPBookit***, uma solução voltada para gerenciamento de agendamentos e reservas.

A falha permite que usuários **não autenticados** realizem ***upload* arbitrário de arquivos** diretamente no servidor *web*, explorando o *endpoint* público da **API REST** do *WordPress*:
/wp-json/bookit/v1/upload-file.

A simplicidade da exploração, aliada ao impacto de comprometimento total do ambiente *WordPress*, faz com que a **CVE-2025-6058** seja considerada de alto risco, principalmente em ambientes expostos à *internet*. A exploração da vulnerabilidade está diretamente alinhada à técnica do **MITRE ATT&CK**:

- ***T1190 – Exploit Public-Facing Application***, por permitir acesso inicial via exploração de endpoint público.

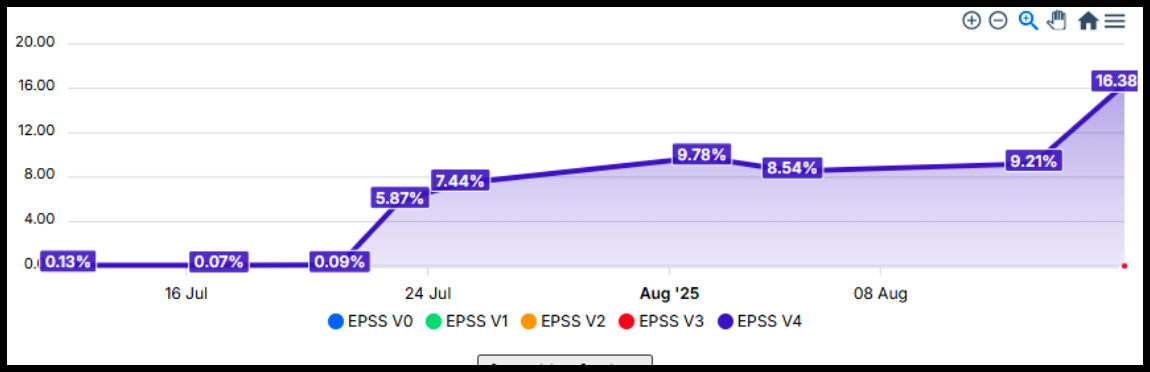

Figura 1 – Probabilidade de Exploração (EPSS) – CVE-2025-6058.

O índice **EPSS** da CVE-2025-6058 demonstra crescimento acelerado na probabilidade de exploração, saindo de menos de **1% em julho** para **16,38% em agosto**. Essa evolução reforça o alto interesse de agentes de ameaça e a urgência na aplicação de medidas de mitigação.

2.2 SISTEMAS, SEGMENTOS E PRODUTOS AFETADOS

A vulnerabilidade afeta especificamente o plugin ***WPBookit***, utilizado por sites *WordPress* para gerenciamento de agendamentos e reservas.

Versões afetadas:

- Até a versão **1.0.4** (**inclusive**).

Condições de risco adicional:

- Instâncias *WordPress* com o *plugin* ativo e expostas diretamente à *internet*;
- Falta de validação de *inputs* na camada de aplicação;
- Ambientes que utilizam o *plugin* como base principal para controle de reservas e serviços.
- Ausência de validação em *uploads* de arquivos e chamadas à **API REST** do *WordPress*;

Segmentos potencialmente impactados:

- **Serviços de agendamento *online***: empresas que utilizam o *plugin* para marcação de horários ou reservas podem sofrer indisponibilidade ou perda de dados;
- ***E-commerce* e plataformas de reservas:** ambientes que dependem da disponibilidade e integridade do sistema de agendamento podem sofrer sequestro, adulteração de dados e indisponibilidade por execução de código malicioso.
- **Pequenas e médias empresas (PMEs)**: geralmente mais suscetíveis por manterem versões desatualizadas e não aplicarem monitoramento robusto em **APIs** e *uploads*.

Organizações que utilizam o ***WPBookit*** em produção devem realizar a **atualização imediata para a versão corrigida (1.0.5)** ou considerar sua **desativação temporária** até que medidas de mitigação adicionais sejam aplicadas. Recomenda-se ainda a adoção de **WAF**, monitoramento de *uploads* e auditoria em diretórios acessíveis externamente.

3. TÁTICO

3.1 VISÃO GERAL DO WORDPRESS E DO PLUGIN WPBOOKIT

O ***WordPress*** é uma das plataformas de gerenciamento de conteúdo (**CMS**) mais utilizadas no mundo para construção de *sites*, *e-commerces* e aplicações *web*. Sua arquitetura modular permite a extensão de funcionalidades por meio de ***plugins***, que interagem diretamente com o núcleo do sistema por meio de *hooks*, *filters* e chamadas assíncronas baseadas na **REST API**.

Dentre os diversos *plugins* disponíveis no ecossistema *WordPress*, o ***WPBookit*** é amplamente utilizado para **agendamento de compromissos e reservas online**. Ele fornece um sistema completo de gerenciamento de horários, serviços e formulários de agendamento, integrado à interface do site. Parte dessas funcionalidades — como o upload de arquivos — é exposta ao *frontend* por meio de ***endpoints*** **REST personalizados**.

A **API REST** do *WordPress* opera a partir do *namespace* **/wp-json/**, permitindo que *plugins* exponham rotas específicas capazes de processar requisições assíncronas (***POST***, ***GET***, ***DELETE*** etc.). Essas rotas podem ser registradas com ou sem autenticação, dependendo da lógica definida pelo desenvolvedor.

No caso do ***WPBookit***, a rota vulnerável é:

```
/wp-json/bookit/v1/upload-file
```

Essa rota foi configurada para aceitar **uploads de arquivos diretamente do cliente**, sem exigir autenticação nem validar adequadamente o tipo e a extensão dos arquivos enviados. Esse cenário permite que um atacante remoto carregue *scripts* **.php** em diretórios acessíveis publicamente no servidor, possibilitando sua execução e resultando em **execução remota de código (RCE)**.

Esse tipo de exposição direta de funcionalidades sensíveis via **REST API**, sem controles apropriados, amplia a superfície de ataque e representa um risco crítico em ambientes que utilizam o *plugin* em produção.

3.2 CONDIÇÕES PARA EXPLORAÇÃO DA VULNERABILIDADE

A seguir, são descritas as principais condições que tornam uma instalação *WordPress* vulnerável à exploração da CVE-2025-6058, considerando o uso do *plugin* ***WPBookit***:

Condição	Descrição
Exposição da rota /wp-json/bookit/v1/upload-file sem autenticação	O *endpoint* **REST** foi registrado sem exigir autenticação, permitindo que qualquer visitante realize chamadas diretamente.
Ausência de validação no *upload* de arquivos	O plugin não implementa verificação de tipo, origem ou extensão dos arquivos enviados, aceitando arquivos **.php** maliciosos.

Plugin ativo em versão vulnerável (≤ 1.0.4)	A falha está presente apenas até a versão **1.0.4**, corrigida posteriormente na versão **1.0.5**.
Acesso público à API REST	O namespace **/wp-json/** está acessível diretamente pela internet, sem restrições adicionais.
Diretórios de *upload* acessíveis via web	Arquivos enviados podem ser gravados em diretórios expostos publicamente, permitindo a execução remota de scripts maliciosos.
Ausência de controles adicionais no servidor	Falta de mitigação em nível de servidor, como regras em **.htaccess**, **mod_security** ou filtros **WAF**.

Tabela 1 - Condição de Exploração

4. OPERACIONAL

4.1 EMULAÇÃO DA VULNERABILIDADE

A exploração da **CVE-2025-6058** pode ser simulada em laboratório por meio de requisições HTTP enviadas ao *endpoint* público do *plugin* ***WPBookit***:

```
/wp-json/bookit/v1/upload-file
```

Esse endpoint aceita requisições **POST** contendo arquivos, sem exigir autenticação ou validar o tipo de conteúdo.

Um atacante remoto pode explorar a falha enviando um arquivo .php malicioso, como no exemplo:

```
curl -i -X POST http://<alvo>/wp-json/bookit/v1/upload-file \
 -F "file=@shell.php"
```

Se o servidor gravar o arquivo em um diretório acessível pela *web*, o atacante poderá acessá-lo via navegador ou ferramentas como ***curl***, obtendo execução remota de código (RCE):

```
curl http://<alvo>/wp-content/uploads/2025/07/shell.php?cmd=id
```

Esse fluxo demonstra o risco de **comprometimento total do ambiente *WordPress*** em instâncias vulneráveis.

4.2 POSSIBILIDADES DE DETECÇÃO

A detecção da exploração da **CVE-2025-6058** pode ser conduzida a partir de:

- Análise de logs de aplicação ou servidor *web*, **verificando chamadas suspeitas ao *endpoint* */wp-json/bookit/v1/upload-file*;**
- Monitoramento de *uploads* incomuns **em diretórios acessíveis pela *web*, especialmente arquivos com extensão *.php*;**
- Soluções de segurança **como WAF, EDR ou NDR, capazes de inspecionar tráfego HTTP em *busca de uploads* maliciosos.**

Condição	Descrição
Método HTTP	**POST**
Rota	**/wp-json/bookit/v1/upload-file**
Arquivos enviados	**Upload de .php ou extensões não previstas pelo plugin**
Origem	**Requisições externas não autenticadas**

Tabela 2 - Campos viáveis para detecção

4.3 MITIGAÇÃO

A mitigação da **CVE-2025-6058** deve ser tratada com prioridade, principalmente em ambientes WordPress expostos à internet.

Correção imediata

- Atualizar o plugin **WPBookit** para a versão **1.0.5** ou superior, na qual a falha foi corrigida;
- Revisar o diretório **/wp-content/uploads/** para identificar e remover arquivos maliciosos já enviados.

Mitigação temporária

- Restringir a execução de arquivos **PHP** no diretório de *uploads*, por exemplo, via .htaccess:

```
<FilesMatch "\.php$">
  Deny from all
</FilesMatch>
```

- Implementar regras em **WAFs (como ModSecurity)** para bloquear *uploads* com extensões não permitidas;
- Criar alertas em **IDS/IPS (ex: Suricata)** para requisições **POST** contendo arquivos **.php** no *endpoint* vulnerável.

Ações defensivas adicionais

- Monitorar continuamente o diretório de *uploads* para criação de arquivos inesperados;
- Adotar *plugins* de segurança como ***Wordfence*** ou ***iThemes Security***, que adicionam camadas de ***hardening***;
- Revisar *endpoints* **REST** expostos pelo *WordPress* para garantir que operações críticas exijam autenticação e validação de parâmetros.

5. CONCLUSÃO

A CVE-2025-6058 evidencia os riscos de *upload* arbitrário em aplicações *WordPress* que não implementam validações adequadas em *endpoints* acessíveis a usuários não autenticados. A falha, presente no plugin **WPBookit até a versão 1.0.4**, permite que qualquer atacante remoto envie arquivos PHP diretamente para o servidor, resultando em **execução de código arbitrário** e no **comprometimento total da aplicação**.

Na prática, a exploração é trivial: um adversário pode enviar um *webshell* e, a partir dele, manipular o site, roubar informações sensíveis ou instalar *backdoors* para garantir persistência. Esse cenário demonstra como funcionalidades comuns — como a criação de tipos de agendamento — podem ser abusadas quando não há uma verificação robusta de autenticação, autorização e validação de conteúdo.

A correção está disponível em versões posteriores do *plugin*, e a **atualização imediata** é a principal medida de mitigação. Além disso, recomenda-se aplicar controles adicionais, como WAF e monitoramento de diretórios sensíveis (ex.: /wp-content/uploads/), para identificar tentativas de exploração. Esse caso reforça a necessidade de **atenção redobrada com *plugins* de terceiros em ambientes *WordPress***, já que uma falha simples pode resultar no comprometimento completo da aplicação.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **MITRE ATT&CK**
- **NIST**
- **CVEFIND**

AUTORES

Gustavo Jatene de Oliveira – Threat Researcher

heimdall
security research
A DIVISION OF ISH