BOLETIM DE SEGURANÇA

Falha crítica no PHP permite execução remota de código em sistemas Windows

heimdall
security research
A DIVISION OF ISH

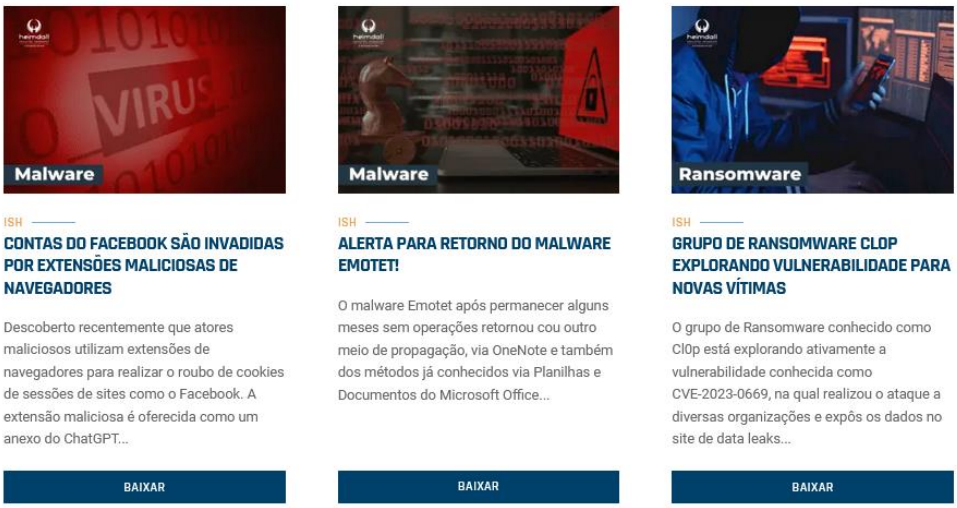
TLP: CLEAR

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

Uma nova falha de segurança CVE-2024-4577 classificada como crítica, foi descoberta no PHP, que pode ser explorada para execução remota de código em certas condições. Devido à ampla utilização do PHP no ecossistema web e à facilidade de exploração essa vulnerabilidade requer uma notável atenção.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-4577 trata-se de uma falha de execução remota de código no PHP, se o sistema estiver configurado para usar certas páginas de código, o Windows pode usar o comportamento "Best-Fit" para substituir caracteres na linha de comando fornecida para funções da API do Win32. O módulo PHP CGI pode interpretar erroneamente esses caracteres como opções do PHP, o que pode permitir que um usuário mal-intencionado passe opções para o binário PHP que está sendo executado e, assim, revele o código-fonte dos scripts, execute código PHP arbitrário no servidor, etc.

Essa vulnerabilidade afeta todas as versões do PHP instaladas no sistema operacional Windows:

- *PHP 8.3 < 8.3.8*
- *PHP 8.2 < 8.2.20*
- *PHP 8.1 < 8.1.29*

Até o momento, foi verificado que, quando o Windows está rodando nos seguintes locais, um atacante não autorizado pode executar diretamente código arbitrário no servidor remoto:

- Chinês Tradicional (Code Page 950)
- Chinês Simplificado (Code Page 936)
- Japonês (Code Page 932)

Para Windows rodando em outros locais, como Inglês, Coreano e Europeu Ocidental, devido à ampla gama de cenários de uso do PHP, atualmente não é possível enumerar e eliminar completamente todos os cenários de exploração potenciais. Portanto, recomenda-se que os usuários realizem uma avaliação abrangente de ativos, verifiquem seus cenários de uso e atualizem o PHP para a versão mais recente para garantir a segurança.

Ao configurar a diretiva Action para mapear solicitações HTTP correspondentes a um binário executável PHP-CGI no Apache HTTP Server, essa vulnerabilidade pode ser explorada diretamente. Configurações comuns afetadas incluem, mas não se limitam a:

```
AddHandler cgi-script .php
Action cgi-script "/cgi-bin/php-cgi.exe"
```

Figura 1 – Configurações comuns afetadas.

```
<FilesMatch "\.php$">
    SetHandler application/x-httpd-php-cgi
</FilesMatch>

Action application/x-httpd-php-cgi "/php-cgi/php-cgi.exe"
```

Figura 2 – Outras configurações comuns afetadas.

3 RECOMENDAÇÕES

Recomenda-se fortemente que todos os usuários atualizem para as versões mais recentes do PHP: **8.3.8**, **8.2.20** e **8.1.29**. Para sistemas que não podem ser atualizados, as seguintes instruções podem ser usadas para mitigar temporariamente a vulnerabilidade.

No entanto, como o PHP CGI é uma arquitetura desatualizada e problemática, ainda é recomendado avaliar a possibilidade de migrar para uma arquitetura mais segura, como **Mod-PHP**, **FastCGI** ou **PHP-FPM**.

- Para usuários que não podem atualizar o PHP: As seguintes regras de reescrita podem ser usadas para bloquear ataques. Observe que essas regras são apenas uma mitigação temporária para os locais em Chinês Tradicional, Chinês Simplificado e Japonês. Ainda é recomendado atualizar para uma versão corrigida ou migrar a arquitetura na prática.
- Para usuários que usam XAMPP para Windows: O XAMPP ainda não lançou arquivos de atualização correspondentes para essa vulnerabilidade no momento da redação deste artigo. Se você confirmar que não precisa do recurso PHP CGI, pode evitar a exposição à vulnerabilidade modificando a seguinte configuração do servidor HTTP Apache, em **C:/xampp/apache/conf/extra/httpd-xampp.conf**.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Devco
- Thehackernews
- NVD

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH