Your IT Company

Principais Vulnerabilidades e Ameaças (Janeiro/25)

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Vulnerabilidades e Ameaças descobertas

2.1. Vulnerabilidade em plug-in popular do WordPress expõe mais de 3 milhões de sites a ataques de injeção de código

Uma vulnerabilidade crítica foi identificada no popular plugin UpdraftPlus: WP Backup & Migration, potencialmente afetando mais de 3 milhões de sites WordPress. Essa falha de segurança permite que invasores não autenticados explorem uma vulnerabilidade de injeção de objetos PHP por meio da desserialização de entradas não confiáveis. O problema afeta a versão 1.23.8 até a versão 1.24.11 do plug-in. Um patch foi lançado para a versão 1.24.12 no intuito de lidar com esse risco significativo.

A vulnerabilidade identificada como CVE-2024-10957, foi classificada pela Wordfence com uma pontuação de alto risco CVSS 3.1:8.8 e possui a seguinte descrição. “O plug-in UpdraftPlus: WP Backup & Migration Plugin para WordPress é vulnerável à injeção de objetos PHP em todas as versões de 1.23.8 a 1.24.11 por meio da desserialização de entrada não confiável na função 'recursive_unserialized_replace'. Isso possibilita que invasores não autenticados injetem um objeto PHP. Nenhuma cadeia POP conhecida está presente no software vulnerável, o que significa que essa vulnerabilidade não tem impacto, a menos que outro plug-in ou tema contendo uma cadeia POP esteja instalado no site. Se uma cadeia POP estiver presente por meio de um plug-in ou tema adicional instalado no sistema de destino, ela poderá permitir que o invasor execute ações como excluir arquivos arbitrários, recuperar dados confidenciais ou executar código, dependendo da cadeia POP presente. Um administrador deve executar uma ação de pesquisa e substituição para acionar a exploração”. A CVE-2024-10957 ainda não foi avaliada pela NIST.

Exploração

É importante enfatizar que, até o momento, nenhuma cadeia conhecida de Prova de Conceito (PoC) foi identificada no software vulnerável. Entretanto, a existência de vulnerabilidades adicionais em plug-ins ou temas complementares pode amplificar consideravelmente os riscos associados a esta falha. De acordo com uma análise de pesquisadores, no relatório da Wordfence, a exploração dessa vulnerabilidade depende de uma ação específica realizada pelo administrador, envolvendo a funcionalidade de "pesquisa e substituição", que atua como o gatilho para o ataque.

Quando explorada, essa vulnerabilidade pode ter sérias consequências, incluindo a exclusão não autorizada de arquivos, o acesso a dados confidenciais dos usuários e a execução remota de código. Este caso reforça a importância de realizar atualizações regulares e de manter uma vigilância proativa na gestão das instalações do WordPress.

Mitigação e Prevenção

Os proprietários de sites que utilizam o plug-in UpdraftPlus devem adotar imediatamente medidas para mitigar essa vulnerabilidade. A solução recomendada é simples e eficaz: atualize o plug-in para a versão 1.24.12 ou qualquer versão subsequente corrigida. A atualização rápida dos

plug-ins por meio do painel do WordPress minimiza significativamente o risco de exposição a ataques, proporcionando uma defesa ágil e eficiente.

Além disso, é fundamental que administradores de sites realizem uma revisão completa das instalações do WordPress, incluindo todos os plug-ins ativos, para identificar e corrigir possíveis vulnerabilidades. Manter todos os componentes de software atualizados é crucial para garantir a segurança e a integridade da presença online.

À medida que o ambiente digital se transforma, as ameaças de cibercriminosos também se adaptam. Estar constantemente atualizado sobre vulnerabilidades como a CVE-2024-10957 e tomar ações imediatas para implementar as correções adequadas são medidas cruciais para prevenir brechas de segurança de alto risco.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://gbhackers.com/wordpress-plugin-vulnerability/ e https://nvd.nist.gov/vuln/detail/CVE-2024-10957

2.2. Lançada correção de vulnerabilidade no kernel Linux que afeta o gerenciamento de liberação de programa e links BPF

Uma vulnerabilidade relacionada à gestão de memória do BPF no Kernel do Linux foi corrigida para evitar situações de "uso após liberação" (use-after-free).

A vulnerabilidade identificada como CVE-2024-56786 foi classificada pela NIST com uma pontuação de nível médio CVSS:3.1:5.5 e possui a seguinte descrição. “Os programas BPF subjacentes ao bpf_link deve ser considerados acessíveis através da cadeia de dependência: gancho de fixação -> link -> programa BPF. Isso implica que, enquanto a memória do link não estiver completamente segura para liberação, existe o risco de o gancho de fixação manter um ponteiro para o programa BPF e acessá-lo indevidamente.”

Exploração

Por padrão, o método bpf_prog_put() é chamado antecipadamente para liberar o programa BPF. Essa abordagem funciona na maioria dos casos devido à espera por um Grace Period (GP) da Read-Copy-Update (RCU) antes da liberação. Contudo, foi identificado que o programa BPF pode ser gerenciado de forma não bloqueante (dependente apenas do GP "clássico"), enquanto o gancho de fixação do link pode exigir proteção adicional da RCU Tasks Trace. Para esses casos, o link BPF deve aguardar a conclusão de ambos os períodos — RCU Tasks Trace e RCU clássico — antes de ser desalocado. Caso contrário, liberar o programa BPF antes do link pode resultar em cenários de uso após liberação.

Mitigação e Prevenção

O patch corrige essa vulnerabilidade adiando a chamada de bpf_prog_put() até que o sistema esteja pronto para desalocar o link BPF. Embora isso possa introduzir um pequeno atraso adicional na liberação do programa (um GP RCU extra), o impacto é considerado mínimo e aceitável.

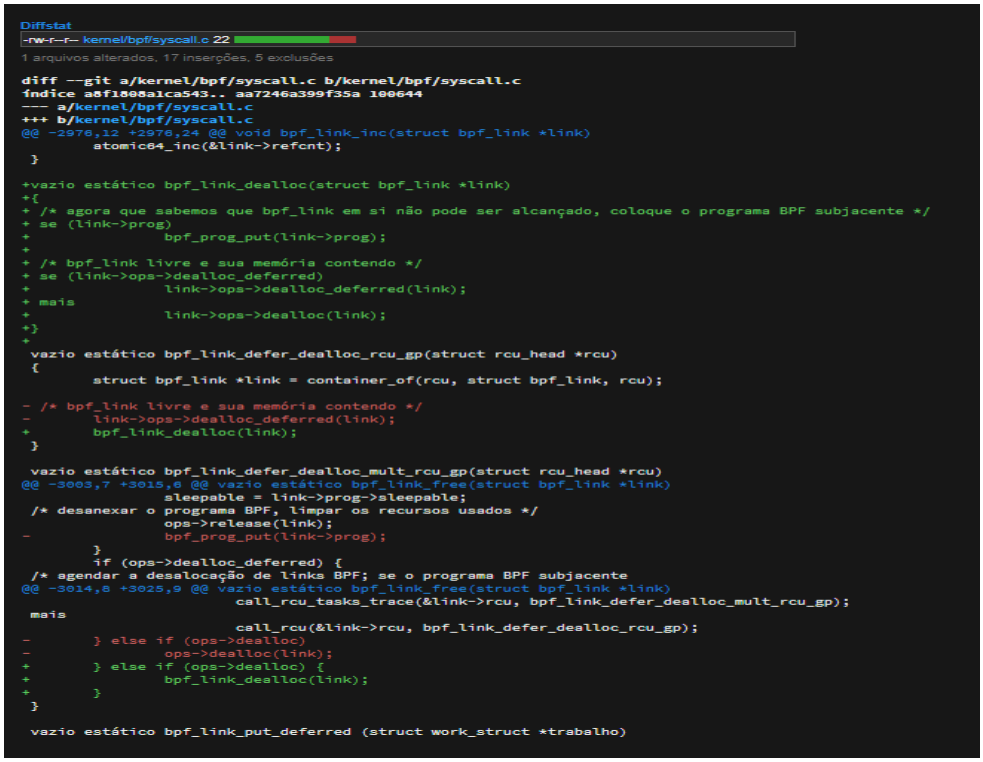
Alternativamente, seria necessário implementar mecanismos mais complexos para rastrear a relação entre ganchos, links e programas BPF, o que foi considerado desnecessário.

Impacto e Otimizações

Para a maioria dos links BPF, o comportamento permanece inalterado, com o bpf_prog_put() e a desalocação do link ocorrendo imediatamente.

Apenas os links que utilizam desalocação adiada podem notar um atraso mínimo na liberação dos programas BPF.

Para reduzir duplicação de código e lógica, a funcionalidade de liberação foi consolidada em um auxiliar chamado bpf_link_dealloc().



```
Diffstat
-rw-r--r-- kernel/bpf/syscall.c 22
1 arquivos alterados, 17 inserções, 5 exclusões

diff --git a/kernel/bpf/syscall.c b/kernel/bpf/syscall.c
índice a8f1808a1ca543..  aa7246a399f35a 100644
--- a/kernel/bpf/syscall.c
+++ b/kernel/bpf/syscall.c
@@ -2976,12 +2976,24 @@ void bpf_link_inc(struct bpf_link *link)
         atomic64_inc(&link->refcnt);
 }

+vazio estático bpf_link_dealloc(struct bpf_link *link)
+{
+ /* agora que sabemos que bpf_link em si não pode ser alcançado, coloque o programa BPF subjacente */
+ se (link->prog)
+                bpf_prog_put(link->prog);
+
+ /* bpf_link livre e sua memória contendo */
+ se (link->ops->dealloc_deferred)
+                link->ops->dealloc_deferred(link);
+ mais
+                link->ops->dealloc(link);
+}
+
 vazio estático bpf_link_defer_dealloc_rcu_gp(struct rcu_head *rcu)
 {
         struct bpf_link *link = container_of(rcu, struct bpf_link, rcu);

- /* bpf_link livre e sua memória contendo */
-        link->ops->dealloc_deferred(link);
+        bpf_link_dealloc(link);
 }

 vazio estático bpf_link_defer_dealloc_mult_rcu_gp(struct rcu_head *rcu)
@@ -3003,7 +3015,6 @@ vazio estático bpf_link_free(struct bpf_link *link)
                 sleepable = link->prog->sleepable;
  /* desanexar o programa BPF, limpar os recursos usados */
                 ops->release(link);
-                bpf_prog_put(link->prog);
         }
         if (ops->dealloc_deferred) {
  /* agendar a desalocação de links BPF; se o programa BPF subjacente
@@ -3014,8 +3025,9 @@ vazio estático bpf_link_free(struct bpf_link *link)
                         call_rcu_tasks_trace(&link->rcu, bpf_link_defer_dealloc_mult_rcu_gp);
 mais
                         call_rcu(&link->rcu, bpf_link_defer_dealloc_rcu_gp);
-        } else if (ops->dealloc)
-                ops->dealloc(link);
+        } else if (ops->dealloc) {
+                bpf_link_dealloc(link);
+        }
 }

 vazio estático bpf_link_put_deferred (struct work_struct *trabalho)
```

Figura 01 – Print do código da correção lançada. Fonte: https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=f44ec8733a8469143fde1984b5e6931b2e2f6f3f

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2024-56786 e https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=f44ec8733a8469143fde1984b5e6931b2e2f6f3f

2.3. Vulnerabilidade do Dell Update Package Framework permite que invasores escalem privilégios.

Uma vulnerabilidade crítica de segurança foi identificada na estrutura do pacote de atualização (DUP) da Dell, potencialmente expondo os sistemas a ataques de escalonamento de privilégios e negação de serviço. A vulnerabilidade identificada como CVE-2025-22395 recebeu pela Dell uma pontuação de nível alto CVSS3.1:8.2 e possui a seguinte descrição “O Dell Update Package Framework, versões anteriores à 22.01.02, contém uma vulnerabilidade de escalonamento de privilégios locais. Um invasor local com poucos privilégios poderia explorar essa vulnerabilidade, levando à execução de scripts remotos arbitrários no servidor. A exploração pode levar a uma negação de serviço por um invasor”. A CVE-2025-22395 ainda não foi avaliada pela NIST.

A falha permite que um invasor local com baixos privilégios explore a estrutura, permitindo a execução de scripts remotos arbitrários no servidor. Isso pode resultar em acesso não autorizado ao

sistema, interrupção de serviços e possível comprometimento de dados confidenciais. A vulnerabilidade decorre do manuseio inadequado de permissões durante os processos de atualização, possibilitando que invasores aumentem seus privilégios.

A Dell reconheceu o problema, mas não divulgou detalhes técnicos específicos sobre o processo de exploração. No entanto, especialistas em segurança enfatizam que essa vulnerabilidade pode ter implicações significativas para organizações que dependem dos mecanismos de atualização da Dell para atualizações de BIOS, firmware e driver.

Exploração

Até o momento, não há evidências públicas de explorações ou provas de conceito disponíveis para essa vulnerabilidade.

Mitigação e Prevenção

A Dell lançou uma versão atualizada do DUP Framework (22.01.02) que resolve o problema. Os usuários são fortemente aconselhados a atualizar para esta versão ou posterior para mitigar os riscos associados ao CVE-2025-22395.

Soluções temporárias

Desativar temporariamente as atualizações automáticas até que os sistemas sejam corrigidos.

Aprimorar a segmentação de rede para limitar os vetores de ataque.

Utilizar sistemas de monitoramento de atividades suspeitas que possam indicar tentativas de exploração.

As organizações que usam sistemas Dell devem priorizar a correção de seus ambientes imediatamente, baixando o DUP Framework mais recente da página de suporte oficial da Dell. O Dell Update Package Framework é amplamente usado em todo o ecossistema da Dell para simplificar as atualizações de BIOS, firmware e drivers de dispositivo. A vulnerabilidade pode, portanto, afetar uma ampla gama de sistemas Dell se não for corrigida.

As equipes de segurança também são incentivadas a implementar ferramentas de monitoramento robustas e seguir as orientações da Dell sobre como lidar com pacotes de atualização com segurança, à medida que as ameaças cibernéticas evoluem, a ação oportuna é crucial para mitigar vulnerabilidades como CVE-2025-22395. As organizações devem permanecer vigilantes, mantendo o software atualizado e aderindo às práticas de segurança recomendadas.

Para mais detalhes sobre a vulnerabilidade acesse os seguintes links abaixo: https://nvd.nist.gov/vuln/detail/CVE-2025-22395

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada quinzenalmente.

Produzido por: Comitê Editorial de Segurança da Service Sec