As vulnerabilidades na plataforma Sitecore CMS permitem o código arbitra

Data: 2025-08-31 16:08:49

Autor: Inteligência Against Invaders

Pesquisadores de segurança da WatchTowr Labs descobriram uma cadeia devastadora de

vulnerabilidades na plataforma de experiência Sitecore que poderia permitir que os invasores

comprometa completamente os sites corporativos sem autenticação.

A pesquisa revela como os cibercriminosos podem envenenar os sistemas de cache do site, escalar privilégios e executar o código remoto em sistemas usados ??por milhares de organizações em todo o mundo.

O envenenamento de cache HTML permite ataques

A vulnerabilidade mais preocupante, designada CVE-2025-53693, centra-se em um Envenenamento por cache HTML técnica que não requer credenciais do usuário para executar.

Os pesquisadores descobriram que poderiam explorar mecanismos de reflexão insegura no XamlPageHandlerFactory da Sitecore para manipular o conteúdo do site em cache, permitindo efetivamente que os invasores injetassem código malicioso em páginas legítimas visualizadas por visitantes desavisados.

O ataque funciona visando o sistema de cache da Sitecore através de um caminho anteriormente esquecido no manipulador XAML da plataforma.

Ao criar solicitações HTTP específicas para o endpoint “/-/xaml/”, os invasores podem invocar o método AddTocache para substituir o conteúdo HTML em cache legítimo com cargas úteis maliciosas.

Essa técnica é particularmente perigosa porque afeta o conteúdo real servido aos visitantes do site, tornando a detecção extremamente difícil.

Os principais aspectos da vulnerabilidade de envenenamento por cache incluem:

- **Autenticação zero necessária** – Os invasores podem explorar essa vulnerabilidade sem nenhuma credenciais válidas.
- **Manipulação de conteúdo direto** – O HTML malicioso pode substituir o conteúdo em cache legítimo servido aos usuários.
- **Operação furtiva** – O cache envenenado parece funcionar normalmente, tornando a detecção desafiadora.
- **Potencial de impacto generalizado** – Qualquer conteúdo em cache nas instâncias afetadas do Sitecore se torna um alvo em potencial.

O que torna essa vulnerabilidade especialmente severa é a facilidade com que as teclas de cache podem ser enumeradas quando a API do Sitecore Itservice é exposta à Internet – uma configuração que os pesquisadores acharam surpreendentemente comum.

Quando essa API estiver acessível, os invasores podem identificar sistematicamente todos os itens em cache em um site e suas chaves de cache associadas, transformando o que pode ser um ataque cego em um ataque precisamente direcionado.

Mesmo em ambientes restritos, os pesquisadores desenvolveram técnicas para chaves de cache de força bruta por meio de ataques de tempo e análise de resposta.

RCE por meio de falhas de desserialização

Com base na capacidade de envenenamento por cache, os pesquisadores identificaram uma vulnerabilidade de execução de código remoto pós-autenticação (CVE-2025-53691) que completa a cadeia de ataques.

Essa falha explora a desertalização insegura no pipeline ConverttoruntimeHtml da Sitecore, onde controlado pelo usuário Conteúdo HTML é processado sem validação de segurança adequada.

A vulnerabilidade reside no uso do Sitecore do Formatter binário inseguro para deseralizar objetos codificados por Base64 incorporados no conteúdo HTML.

Os invasores podem criar HTML maliciosos contendo aparelhos de desserialização codificados especialmente que, quando processados ??pelo pipeline vulnerável, executam o código arbitrário no servidor de destino.

O ataque pode ser acionado pela funcionalidade do editor de conteúdo da Sitecore, exigindo apenas privilégios básicos de edição de conteúdo, em vez de acesso administrativo completo.

Particularmente preocupante é que esse coletor de desserialização parece ser um problema herdado que o Sitecore tentou abordar removendo rotas acessíveis ao código vulnerável, em vez de corrigir a falha de segurança subjacente.

A pesquisa WatchTowr demonstra que ainda existem caminhos alternativos para acionar essa vulnerabilidade, deixando os sistemas expostos mesmo após as atualizações anteriores de segurança.

Linha do tempo de impacto crítico

As vulnerabilidades afetam a plataforma de experiência do Sitecore versão 10.4.1 e versões potencialmente anteriores, impactando cerca de 22.000 instâncias do Sitecore em todo o mundo, de acordo com os dados de digitalização da Internet.

Os sistemas afetados incluem sites operados pelas principais empresas de várias indústrias, tornando substancial o impacto potencial.

Sitecore respondeu Prontamente para a divulgação, liberando patches em junho e julho de 2025, depois de receber os relatórios de vulnerabilidade em fevereiro e março.

No entanto, a linha do tempo prolongada entre a descoberta e o patch destaca a complexidade de abordar falhas de segurança profundamente incorporadas nos sistemas de gerenciamento de conteúdo corporativo.

A pesquisa enfatiza uma tendência preocupante, onde as vulnerabilidades de segurança em plataformas corporativas populares podem criar efeitos em cascata em milhares de organizações.

A combinação de envenenamento por cache de pré-autenticação com a execução do código pós-autenticação representa um cenário completo de compromisso que poderia permitir que os invasores estabeleçam acesso persistente a ambientes de destino.

As organizações que usam a plataforma de experiência do Sitecore devem verificar imediatamente que aplicaram os patches de segurança mais recentes e revisar suas configurações de API de serviços itens para garantir que não sejam desnecessariamente expostos a ataques baseados na Internet.

A descoberta serve como um lembrete gritante da importância das avaliações regulares de segurança para os componentes críticos de infraestrutura corporativa.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**