Patches Sitecore do provedor de CMS explorados dia zero crítico - Agains

Data: 2025-09-06 12:51:17

Autor: Inteligência Against Invaders

Analistas de segurança da equipe Mandiant Threat Defense interromperam um ataque que explorava uma vulnerabilidade de dia zero no Sitecore, um popular sistema de gerenciamento de conteúdo (CMS) usado por empresas como HSBC, L'Oréal, Toyota e United Airlines.

Em um relatório publicado em 3 de setembro, a Mandiant, parte do Google Cloud, disse que o ataque aproveitou as chaves de máquina ASP.NET expostas nos guias de implantação do Sitecore de 2017 e anteriores para realizar a execução remota de código (RCE).

ASP.NET é uma estrutura de aplicativo da Web desenvolvida pela Microsoft para criar sites dinâmicos, aplicativos da Web e APIs (interfaces de programação de aplicativos). ASP.NET chaves de máquina são chaves criptográficas usadas para proteger operações críticas em aplicativos ASP.NET.

Essas chaves de máquina foram expostas devido a uma vulnerabilidade de desserialização do ViewState no Sitecore Experience Manager (XM) e no Sitecore Experience Platform (XP).

Ryan Dewhurst, chefe de inteligência proativa de ameaças da WatchTowr, comentou: "O problema decorre de usuários do Sitecore copiando e colando chaves de exemplo da documentação oficial, em vez de gerar chaves únicas e aleatórias – um movimento que não recomendamos".

A Mandiant relatou a falha ao Sitecore. Wiz, uma autoridade de numeração (CNA) de vulnerabilidades e exposições comuns (CVE), divulgou-o publicamente em 3 de setembro como CVE-2025-53690, com uma classificação de pontuação de gravidade (CVSS) de 9,0 (crítico).

Quando explorado, o CVE-2025-53690 permite a injeção de código no Sitecore XM e Sitecore XP até a versão 9.0.

A Mandiant afirmou que a vulnerabilidade afeta os clientes que implantaram qualquer versão de vários produtos Sitecore usando a chave de amostra exposta nos guias de implantação disponíveis publicamente (especificamente Sitecore XP 9.0 e Active Directory 1.4 e versões anteriores).

Cadeia de ataque explorando a falha do Sitecore

A equipe de resposta rápida da Mandiant interrompeu o ataque antes que seu ciclo de vida completo pudesse ser observado, mas a investigação ainda descobriu as principais táticas do adversário.

O agente da ameaça demonstrou conhecimento sofisticado do produto visado e suas vulnerabilidades, executando uma cadeia de ataque metódica:

1. **Acesso inicial:** Explorou o CVE-2025-53690 em uma instância Sitecore voltada para a Internet, alcançando RCE
2. **Reconhecimento e roubo de dados:** Implantou o malware WEEPSTEEL por meio de uma carga útil ViewState descriptografada para reconhecimento interno; arquivou o diretório raiz do aplicativo Web, provavelmente visando arquivos confidenciais, como *web.config*; Reconhecimento de host e rede conduzido
3. **Persistência:** Ferramentas adicionais colocadas em um diretório público, incluindo EARTHWORM (tunelamento de rede de código aberto), DWAGENT (trojan de acesso remoto de código aberto) e SHARPHOUND (reconhecimento AD de código aberto)
4. **Escalonamento de privilégios e movimento lateral:** Criou contas de administrador local e despejou hives SAM/SYSTEM para coletar credenciais em cache; usou RDP para movimento lateral após comprometimento de credenciais; persistência mantida via DWAGENT durante a realização do reconhecimento do Active Directory

Impacto do ataque ainda desconhecido

A Sitecore informou à Mandiant que suas implantações mais recentes agora geram automaticamente chaves de máquina exclusivas e os clientes afetados foram notificados.

O provedor de CMS também lançou Um aviso de segurança em 3 de setembro, aconselhando seus clientes sobre como mitigar essa ameaça.

Caitlin Condon, vice-presidente de pesquisa de segurança da VulnCheck, disse que esse ataque é outra evidência de que “os agentes de ameaças definitivamente leem a documentação”.

“A vulnerabilidade de dia zero surge tanto da própria configuração insegura (ou seja, uso da chave estática da máquina) quanto da exposição pública. Os defensores que suspeitarem que possam ser afetados devem girar as chaves de suas máquinas imediatamente e garantir, sempre que possível, que suas instalações Sitecore não sejam expostas à Internet pública”, aconselhou.

No entanto, ela também destacou que girar as chaves e bloquear as configurações não são suficientes por si só se os agentes de ameaças conseguirem obter acesso à rede de uma organização.

“As equipes de segurança e caça a ameaças precisarão examinar os ambientes em busca de sinais de comprometimento, principalmente porque a investigação da Mandiant descobriu que o agente da ameaça havia implantado malware e ferramentas adicionais voltadas para reconhecimento interno e persistência em um ou mais ambientes comprometidos”, acrescentou.

Dewhurst, da WatchTowr, disse que, nesta fase, o raio de explosão do ataque permanece desconhecido.

“Mas esse bug exibe todas as características que normalmente definem vulnerabilidades graves. O impacto mais amplo ainda não veio à tona, mas vai “, argumentou.

Este novo ataque ocorre três meses depois que o WatchTowrrevelou sete vulnerabilidades no

Sitecore produtos que poderiam ser encadeados em um ataque em larga escala.