CISA diz que hackers violaram agência federal usando exploração do Geo

Data: 2025-09-23 19:27:44

Autor: Inteligência Against Invaders

A CISA revelou que os invasores violaram a rede de uma agência não identificada do Poder

Executivo Civil Federal dos EUA (FCEB) no ano passado, depois de comprometer uma instância do

GeoServer não corrigida.

O bug de segurança (rastreado como CVE-2024-36401) é uma vulnerabilidade crítica de execução remota de código (RCE) corrigida em 18 de junho de 2024. A CISA adicionou a falha ao seu catálogo de vulnerabilidades exploradas ativamente cerca de um mês depois, depois que vários pesquisadores de segurança compartilharam explorações de prova de conceito online [1, 2, 3], demonstrando como obter execução de código em servidores expostos.

Embora a agência de segurança cibernética não tenha fornecido detalhes sobre como as falhas estavam sendo exploradas, o serviço de monitoramento de ameaças Shadowserver observou ataques CVE-2024-36401 a partir de 9 de julho de 2024, enquanto o mecanismo de busca OSINT ZoomEye estava rastreando mais de 16.000 servidores GeoServer que foram expostos online.

Dois dias após a detecção dos primeiros ataques, os agentes de ameaças obtiveram acesso ao servidor GeoServer de uma agência federal dos EUA e comprometeram outro cerca de duas semanas depois. No próximo estágio do ataque, eles se moveram lateralmente pela rede da agência, violando um servidor web e um servidor SQL.

“Em cada servidor, eles carregaram (ou tentaram carregar) shells da web, como o China Chopper, juntamente com scripts projetados para acesso remoto, persistência, execução de comandos e escalonamento de privilégios”, CISA ele disse em um aviso de terça-feira.

“Uma vez dentro da rede da organização, os agentes de ameaças cibernéticas confiaram principalmente em técnicas de força bruta [T1110] para obter senhas para movimento lateral e escalonamento de privilégios. Eles também acessaram contas de serviço explorando seus serviços associados.

Os agentes de ameaças permaneceram sem serem detectados por três semanas até que a ferramenta Endpoint Detection and Response (EDR) da agência federal alertou seu Centro de Operações de Segurança (SOC) sobre a violação, sinalizando um arquivo como suspeito de malware no SQL Server em 31 de julho de 2024.

Depois que a atividade maliciosa dos invasores acionou alertas adicionais de EDR, a equipe do SOC isolou o servidor e iniciou uma investigação com a assistência da CISA.

A CISA agora é Exortando os defensores da rede para agilizar a correção de vulnerabilidades críticas (especialmente aquelas adicionadas ao seu Catálogo de vulnerabilidades exploradas

conhecidas), garantem que os centros de operações de segurança monitorem continuamente os alertas EDR em busca de atividades suspeitas na rede e fortaleçam seus planos de resposta a incidentes.

Em julho, a agência de segurança cibernética dos EUA emitiu outro aviso após um engajamento proativo em uma organização de infraestrutura crítica dos EUA.

Embora não tenha encontrado evidências de atividade maliciosa em sua rede, descobriu muitos riscos de segurança cibernética, incluindo, entre outros, credenciais armazenadas de forma insegura, credenciais de administrador local compartilhadas em várias estações de trabalho, acesso remoto irrestrito para contas de administrador local, registro insuficiente e problemas de configuração de segmentação de rede.

[IMAGEM REMOVIDA]