Alerta de segurança: Vulnerabilidade no Ivanti Endpoint Manager Mobile. C

Data: 2025-09-21 06:43:39

Autor: Inteligência Against Invaders

Redazione RHC**:21 Setembro 2025 08:42**

A Agência de Segurança Cibernética dos EUA (CISA) emitiu um alerta em relação a dois kits de malware descobertos na rede de uma organização não identificada após a exploração de novas vulnerabilidades no **Sistema de gerenciamento de dispositivos móveis Ivanti Endpoint Manager Mobile (EPMM).**

Os invasores exploraram o CVE-2025-4427 e CVE-2025-4428 vulnerabilidades, ambas usadas em ataques de dia zero **antes do lançamento das atualizações da Ivanti em maio de 2025.**

A primeira vulnerabilidade permite **Desvio de autenticação** e acesso a recursos protegidos, enquanto o segundo permite **Execução remota de código**. Juntos, eles permitem a execução não autorizada de comandos arbitrários nos vulneráveis **EPMM** servidor. A CISA observa que *o ataque começou por volta de 15 de maio de 2025, logo após a publicação do exploit PoC.*

Os invasores usaram esse acesso para executar comandos que lhes permitiam coletar informações do sistema, fazer upload de arquivos maliciosos, listar o conteúdo do diretório raiz, realizar reconhecimento de rede, executar um script para criar um despejo de heap e extrair credenciais LDAP. Dois conjuntos diferentes de arquivos maliciosos foram carregados no servidor, ambos no diretório /tmp, cada um garantindo persistência injetando e executando código arbitrário:

Em ambos os casos, o *JAR lançou uma classe Java que agia como um ouvinte HTTP malicioso*. Essas classes interceptaram solicitações específicas, descriptografaram cargas incorporadas e criaram dinamicamente uma nova classe que era executada diretamente na memória.

Especificamente, o **ReflectUtil.class** foi usado para *manipular objetos Java e injetar um componente SecurityHandlerWanListener no tempo de execução do Apache Tomcat.* Esse ouvinte interceptou solicitações HTTP, decodificou e descriptografou os dados e, em seguida, executou a classe gerada.

O segundo componente *(WebAndroidAppInstaller.class)* usou uma chave codificada para descriptografar o parâmetro password da solicitação, que foi usada para gerar e executar a nova classe. O resultado foi então criptografado novamente com a mesma chave e enviado na resposta.

Portanto, ambas as cadeias forneceram um recurso oculto para execução remota de código, presença persistente no sistema e orquestração de estágios de ataque subsequentes, incluindo interceptação e processamento de tráfego HTTP para exfiltração de dados.

A CISA recomenda que os administradores atualizem imediatamente todas as instalações vulneráveis do Ivanti EPMM para a versão mais recente, fortaleçam o monitoramento de atividades e restrinjam o acesso a sistemas MDM para evitar invasões semelhantes no futuro.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli