CISA expõe kits de malware implantados em ataques Ivanti EPMM - Agains

Data: 2025-09-20 00:26:29

Autor: Inteligência Against Invaders

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) publicou uma análise do

malware implantado em ataques que exploram vulnerabilidades que afetam o Ivanti Endpoint

Manager Mobile (EPMM).

As falhas são um desvio de autenticação no componente API do EPMM (CVE-2025-4427) e uma vulnerabilidade de injeção de código (CVE-2025-4428) que permite a execução de código arbitrário.

As duas vulnerabilidades afetam as seguintes ramificações de desenvolvimento do Ivanti EPMM e suas versões anteriores: 11.12.0.4, 12.3.0.1, 12.4.0.1 e 12.5.0.0.

A Ivanti abordou os problemas em 13 de maio, mas os agentes de ameaças já haviam sido explorando-os como dia zeroem ataques contra “um número muito limitado de clientes”.

Cerca de uma semana depois, a plataforma de inteligência de ameaças EclecticIQ denunciado com alta confiança que um grupo de espionagem China-Nexus estava aproveitando as duas vulnerabilidades desde pelo menos 15 de maio.

Os pesquisadores disseram que o agente de ameaças vinculado à China conhece muito bem a arquitetura interna do Ivanti EPMM, sendo capaz de redirecionar componentes do sistema para exfiltrar dados.

O relatório da CISA, no entanto, não faz nenhuma atribuição e se concentra apenas nos detalhes técnicos de arquivos maliciosos obtidos de uma organização atacada por agentes de ameaças usando uma cadeia de exploração para CVE-2025-4427 e CVE-2025-4428.

Dividir a entrega de malware

A agência dos EUA analisou dois conjuntos de malware que consistem em cinco arquivos que os hackers usaram para obter acesso inicial aos sistemas Ivanti EPMM locais.

“Os agentes de ameaças cibernéticas visaram o */mifs/rs/api/v2/* endpoint com solicitações HTTP GET e usou o *?formato*= para enviar comandos remotos maliciosos”, CISA Diz.

Os comandos permitem que o agente da ameaça execute atividades de reconhecimento coletando informações do sistema, listando o diretório raiz, mapeando a rede, buscando arquivos maliciosos e extraindo credenciais do Lightweight Directory Access Protocol (LDAP).

Cada um dos conjuntos de malware analisados incluía um carregador distinto, mas com o mesmo

nome, e ouvintes maliciosos que permitem injetar e executar código arbitrário no sistema comprometido:

- **Conjunto 1**:
  - *web-install.jar* (Carregador 1)
  - *ReflectUtil.class* – incluído no Loader 1, manipula objetos Java para injetar e gerenciar o ouvinte malicioso no conjunto
  - *SecurityHandlerWanListener.class* – ouvinte malicioso que pode ser usado para injetar e executar código no servidor, exfiltrar dados e estabelecer persistência
- **Conjunto 2**:
  - *web-install.jar* (Carregador 2)
  - *WebAndroidAppInstaller.class* – um ouvinte malicioso no Loader 2, que o agente da ameaça poderia usar para injetar e executar código, criar persistência e exfiltrar dados

De acordo com a CISA, o agente da ameaça entregou o malware por meio de solicitações HTTP GET separadas em blocos segmentados codificados em Base64.

Os dois conjuntos distintos de malware funcionam de forma semelhante, interceptando solicitações HTTP específicas para decodificar e executar cargas úteis fornecidas pelos invasores.

A CISA forneceu indicadores detalhados de comprometimento (IOCs), regras YARA e uma regra SIGMA para ajudar as organizações a detectar esses ataques.

A recomendação da agência para as empresas que encontrarem o malware analisado ou arquivos semelhantes em seus sistemas é isolar os hosts afetados, coletar e revisar artefatos e criar uma imagem de disco forense completa para compartilhar com a CISA.

Como ação de mitigação, a CISA recomenda corrigir o Ivanti EPMM afetado imediatamente e tratar os sistemas de gerenciamento de dispositivos móveis (MDM) como ativos de alto valor (HVAs) que exigem restrições de segurança e monitoramento adicionais.

[IMAGEM REMOVIDA]