CISA alerta sobre malware implantado por meio de falhas do Ivanti EPMM

Data: 2025-09-20 14:56:50

Autor: Inteligência Against Invaders

CISA alerta sobre malware implantado por meio de falhas do Ivanti EPMM

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) divulgou duas cepas de malware encontradas em uma rede comprometida por meio de falhas do Ivanti EPMM.

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) publicou detalhes técnicos de duas famílias de malware que foram descobertas na rede de uma organização não identificada após o comprometimento do Ivanti Endpoint Manager Mobile (EPMM).

A CISA divulgou um relatório sobre duas cepas de malware usadas em exploits de falhas do Ivanti EPMM CVE-2025-4427 e CVE-2025-4428.

“A Agência de Segurança Cibernética e Infraestrutura (CISA) obteve dois conjuntos de malware de uma organização comprometida por agentes de ameaças cibernéticas que exploramCVE-2025-4427eCVE-2025-4428
no Ivanti Endpoint Manager Mobile (Ivanti EPMM).” lê o Relatório de análise de malware publicado pela CISA. “Cada conjunto contém carregadores para ouvintes mal-intencionados que permitem que os agentes de ameaças cibernéticas executem código arbitrário no servidor comprometido.”

Em meados de maio, a IvantiLançadoAtualizações de segurança para resolver vulnerabilidadesCVE-2025-4427 e CVE-2025-4428, no software Endpoint Manager Mobile (EPMM). A empresa confirmou que os agentes de ameaças encadearam as falhas em ataques limitados para obter a execução remota de código.

Abaixo está a descrição deles:

- **CVE-2025-4427**(Pontuação CVSS: 5.3) – Um desvio de autenticação no Endpoint Manager Mobile permitindo que invasores acessem recursos protegidos sem as credenciais adequadas.
- **CVE-2025-4428**(Pontuação CVSS: 7.2) – Uma vulnerabilidade de execução remota de código no Endpoint Manager Mobile permitindo que invasores executem código arbitrário no sistema de destino.

O CERT-EU relatou ambas as vulnerabilidades à empresa de software. A empresa confirmou que os agentes de ameaças podem encadear as duas vulnerabilidades para obter a execução remota de código sem autenticação.

As vulnerabilidades foram resolvidas com as versões 11.12.0.5, 12.3.0.2, 12.4.0.2 ou 12.5.0.1.

As vulnerabilidades afetam duas bibliotecas de código aberto sem nome usadas no EPMM, a empresa apontou que elas não residem em seu código. A empresa ainda está investigando os ataques, no entanto, não possui “indicadores atômicos confiáveis” no momento da redação deste artigo.

Em maio, a Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA)AdicionadoGoogle Chromium, roteadores DrayTek e SAP NetWeaver falhas em seuCatálogo de vulnerabilidades exploradas conhecidas (KEV).

Em maio de 2025, os agentes de ameaças exploraram as falhas do Ivanti EPMM para acessar servidores, executando comandos por meio do /mifs/rs/api/v2/ Extremidade. Os invasores realizaram uma série de atividades maliciosas, incluindo coleta de dados do sistema, download de malware e mapeamento de redes. Os invasores despejaram as credenciais LDAP e mantiveram a persistência gravando arquivos maliciosos em /tmp. A CISA analisou dois conjuntos de malware e recomenda que as organizações usem IOCs, apliquem orientações de detecção e atualizem para a versão mais recente do Ivanti EPMM.

Os conjuntos de malware analisados pela CISA são:

- O conjunto 1 consiste nos seguintes arquivos maliciosos:web-install.jar,ReflectUtil.classeSecurityHandlerWanListener.class.
- O conjunto 2 consiste nos seguintes arquivos maliciosos:web-install.jareWebAndroidAppInstaller.class.

Cada conjunto de malware inclui um carregador e um ouvinte que permitem que os invasores injetem e executem código arbitrário no servidor comprometido.

Os carregadores executam um ouvinte de classe Java malicioso, interceptando solicitações HTTP para decodificar e descriptografar cargas úteis para execução.

Abaixo estão detalhes adicionais sobre os dois conjuntos de malware.

Conjunto 1: Usa um carregador (ReflectUtil.class) disfarçado de pacote Apache para contornar restrições e instalar secretamente um ouvinte mal-intencionado (SecurityHandlerWanListener) no Apache Tomcat. Esse ouvinte intercepta solicitações HTTP específicas, descriptografa cargas ocultas e cria dinamicamente novas classes Java. Os invasores podem executar código arbitrário, manter a persistência e exfiltrar dados.

Conjunto 2: Contém um carregador (WebAndroidAppInstaller.class) que se apresenta como um serviço MobileIron. Ele instala outro ouvinte malicioso que intercepta solicitações HTTP codificadas em formulários, descriptografa parâmetros ocultos com uma chave AES codificada, cria e executa novas classes e, em seguida, criptografa e retorna os resultados. Os invasores executam arbitragemary na instância vulnerável e pode roubar dados e assumir o controle de um sistema comprometido.

Ambos os conjuntos de malware oferecem aos invasores recursos poderosos de persistência, execução de código e roubo de dados.

As organizações devem atualizar para a versão mais recente, monitorar atividades suspeitas e restringir o acesso a sistemas MDM para evitar ataques.

A CISA também compartilhou as regras YARA e SIGMA para detectar o malware, juntamente com as técnicas MITRE ATT&CK.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Ivanti EPMM)