Alertas da CISA de hackers direcionados à Ivanti Endpoint Manager Vulne

Data: 2025-09-19 09:31:47

Autor: Inteligência Against Invaders

Os atores de ameaças cibernéticas armaram duas vulnerabilidades críticas de Mobile Mobile

Manager (EPMM)-CVE-2025-4427 e CVE-2025-4428-para implantar carregadores e ouvintes

sofisticados em servidores comprometidos.

O malware consiste em dois conjuntos de componentes: Loader 1 (Web-Install.Jar, RefletUtil.class, SecurityHandlerWanListener.class) e Loader 2 (Web-Install.jar, WebandroidAppInstaller.class), ambos projetados para injetar código arbitrário e manter a persistência no apacho do apacho.

A CISA obteve cinco arquivos de malware de uma organização comprometida via CVE-2025-4427 (desvio de autenticação) e CVE-2025-4428 (injeção de código) no IVANTI EPMM.

Os atacantes exploraram o/MIFS/RS/API/V2/ENDPOND, encadeando solicitações HTTP com um parâmetro de formato para fornecer pedaços codificados por Base64, reconstruir arquivos JAR em/TMP e carregar classes java maliciosas.

Uma vez implantados, essas classes interceptam solicitações HTTP com cabeçalhos ou cargas úteis específicas para decodificar, descriptografar e executar o código arbitrário.

As organizações que executam o IVANTI EPMM versões 11.12.0.4 e anterior, 12.3.0.1 e anterior, 12.4.0.1 e anterior ou 12.5.0.0 e anterior devem atualizar imediatamente.

Ivanti EPMM Versões 11.12.0.4 e anterior, 12.3.0.1 e anterior, 12.4.0.1 e anterior e 12.5.0.0 e anterior. Ivanti lançado Patches e divulgou publicamente as duas vulnerabilidades em 13 de maio de 2025. A CISA adicionou esses CVEs ao seu conhecido catálogo de vulnerabilidades exploradas em 19 de maio de 2025.

Ações -chave

Detecte a atividade, implantando indicadores fornecidos de compromisso (IOCs) e regras de detecção de Yara e Sigma.

Evite a exploração, atualizando para a mais recente liberação de Ivanti EPMM e tratando os sistemas MDM como ativos de alto valor com restrições e monitoramento aumentados.

IOCs para download: mar-251126.r1.v1.clear (Stix 2.0 JSON). As assinaturas de detecção incluem CISA-criada Regras de yara Para carregadores e ouvintes, e uma regra Sigma (AR25-260A/B Sigma Yaml) para identificar solicitações suspeitas HTTP, nomes de classe, hashes de arquivo e artefatos de rede.

O arquivo de jar do carregador 1 hospeda refletiTil.class, que injeta um ouvinte malicioso (SecurityHandlerwanListener) em Apache Tomcat Ao ignorar as restrições do módulo JDK, decodificando uma classe de ouvinte compactada por GZIP, codificada por Base64, e adicionando-a à lista do ouvinte do servlet.

O SecurityHandlerWanListener intercepta solicitações HTTP contendo uma cadeia de passagem específica, cabeçalho do referente e carga útil, depois decodifica e as cargas úteis base64 de decreto de AES para definir e executar novas classes no servidor, permitindo que a execução e a exfiltração de dados do código arbitário.

O arquivo jar do carregador 2 se disfarça de webandroidAppInstaller.class como parte do com.mobileiron.service.

A string base64:

1. Primeiro usasun.misc.BASE64Decoderpara ligardecodeBuffer.
2. Se a primeira tentativa falhar, ele usajava.util.Base64para ligargetDecoder.

O ouvinte valida solicitações com o tipo de conteúdo Aplicativo/x-www-forma-urlcoded, extrai um parâmetro de senha codificado por 64, aes decreta-o, carrega dinamicamente novas classes, criptografa e codifica resultados de execução com a mesma chave e retorna uma resposta MD5-Hashed. Isso permite que os invasores executem código arbitrário e recebam saída de comando.

Os invasores dividiram cada carregador em vários segmentos codificados por Base64 entregues através de solicitações GET separadas para o ponto final do/MIFS/RS/API/V2/FencherUsage. A injeção de linguagem de expressão de Java grava e anexa esses pedaços aos arquivos em /TMP, evitando controles baseados em assinatura e verificações de tamanho de arquivo.

Mitigações

Implante YARA Regras CISA_251126_01 através do CISA_251126_05 para detectar os artefatos de arquivo JAR e classificar combinando padrões exclusivos de hashes e bytes SHA-256.

Alinhe as defesas com CISA e as metas de desempenho da cibersegurança cibernética do NIST, incluindo segmentação de rede, lista de permissões de aplicativos, autenticação multifatorial para interfaces administrativas e revisão regular de log para detectar comandos anômalos ou atividades de arquivo.

Implemente a regra Sigma na Tabela 7 para sinalizar solicitações anormais HTTP GET, atividade de carregamento de classe e IOCs de rede, como IPs maliciosos conhecidos.

Se detectada, a quarentena afetou os hosts, captura imagens forenses, revise os processos de execução e relate incidentes à CISA por meio de seu centro de operações 24/7 ou sistema de relatórios de incidentes. Envie amostras de malware através do formulário de envio de análise de malware da CISA.

Atualize para a mais recente liberação do IVANTI EPMM sem demora. Aplicar restrições aprimoradas e monitoramento contínuo nas plataformas MDM como ativos de alto valor.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.