As vulnerabilidades do Ivanti Endpoint Manager permitem a execução do c

Data: 2025-09-09 18:31:58

Autor: Inteligência Against Invaders

O Ivanti lançou o Security Advisory para o Endpoint Manager Versions 2024 SU3 e 2022 SU8,

detalhando duas falhas de alta severidade (CVE-2025-9712 ??e CVE-2025-9872).

Ambos os problemas decorrem da validação insuficiente do nome do arquivo e exigem apenas uma interação mínima do usuário, potencialmente concedendo controle total sobre os sistemas afetados.

Visão geral da vulnerabilidade

As duas vulnerabilidades compartilham características idênticas e impacto:

Número cve	Descrição	Pontuação do CVSS (gravidade)
CVE-2025-9712	Validação insuficiente do nome do arquivo no Endpoint Manager Antes de 2024 Atualização de segurança SU3 1 e 2022 SU8 Atualização de segurança 2 permite a execução de código não autenticada remota. Requer interação do usuário.	8.8 (alto)
CVE-2025-9872	Igual ao CVE-2025-9712: Validação insuficiente do nome do arquivo permite a execução de código não autenticada remota com a interação do usuário.	8.8 (alto)

Ivanti Nenhuma exploração conhecida dessas vulnerabilidades na natureza no momento da divulgação. No entanto, a alta severidade e a facilidade de exploração sublinham a urgência para os administradores atualizarem os sistemas afetados.

Versões afetadas e remediação

Todas as instalações do Endpoint Manager executando a atualização de segurança 2022 SU8 ou anteriores, bem como 2024 SU3 e anterior, são vulneráveis. Ivanti lançou correções nas seguintes versões:

Nome do produto	Versão afetada (s)	Versão resolvida (s)	Disponibilidade de patch
Ivanti Endpoint Manager	2022 SU8 Atualização de segurança 1 e anterior	2022 SU8 Atualização de segurança 2	Download Disponível no Sistema de Licença Ivanti (ILS)
Ivanti Endpoint Manager	2024 SU3 e anterior	2024 SU3 Atualização de segurança 1	Download Disponível no Sistema de Licença Ivanti (ILS)

Os clientes devem fazer login no sistema de licença Ivanti para recuperar as atualizações necessárias.

A filial de 2022 chegará ao final da vida no final de outubro de 2025. As organizações ainda nessa filial devem não apenas aplicar a atualização de segurança, mas também planejar migrar para uma versão suportada para manter a segurança e o suporte contínuos.

Ações recomendadas

Os administradores são aconselhados a:

1. Verifique a versão do Endpoint Manager implantada em seu ambiente.
2. Faça o download imediatamente e instale a atualização de segurança apropriada no portal ILS.
3. Revise os controles de acesso ao usuário e políticas de terminal para limitar a exposição potencial.
4. Agende os planos de migração para a filial de 2022 para se alinhar com o próximo final da vida em outubro de 2025.

Ao aplicar proativamente essas atualizações e planejamento para migrações de filiais, as organizações podem se defender contra não autorizadas execução de código remoto e defender a integridade de sua infraestrutura de gerenciamento de terminais.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.

Divya

Divya é um jornalista sênior da GBHackers que cobre ataques cibernéticos, ameaças, violações, vulnerabilidades e outros acontecimentos no mundo cibernético.