Várias vulnerabilidades nos produtos Ivanti podem permitir a execução re

Data: 2025-09-13 00:20:06

Autor: Inteligência Against Invaders

Várias vulnerabilidades foram descobertas nos produtos Ivanti, a mais grave das quais pode permitir a execução remota de código. Os detalhes dessas vulnerabilidades são os seguintes:

Tática: Acesso inicial ([TA0001](#)):

Técnica: Explorar aplicativo voltado para o público ([T1190](#)):

- A validação insuficiente do nome de arquivo no Ivanti Endpoint Manager antes da Atualização de Segurança 2024 SU3 1 e da Atualização de Segurança 2022 SU8 permite que um invasor remoto não autenticado obtenha a execução remota de código. A interação do usuário é necessária. (CVE-2025-9712, CVE-2025-9872)

Detalhes de vulnerabilidades de menor gravidade:

- A falta de autorização no Ivanti Connect Secure antes da versão 22.7R2.9 ou 22.8R2, no Ivanti Policy Secure antes da versão 22.7R1.6, no Ivanti ZTA Gateway antes da versão 22.8R2.3-723 e no Ivanti Neurons for Secure Access antes da versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor autenticado remoto com privilégios de administrador somente leitura defina configurações restritas (CVE-2025-8712, CVE-2025-55148, CVE-2025-55144)
- O CSRF no Ivanti Connect Secure antes da versão 22.7R2.9 ou 22.8R2, o Ivanti Policy Secure antes da versão 22.7R1.6, o Ivanti ZTA Gateway anterior à versão 2.8R2.3-723 e o Ivanti Neurons for Secure Access antes da versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor remoto não autenticado execute ações limitadas em nome do usuário vítima. A interação do usuário é necessária. (CVE-2025-8711)
- A falta de autorização no Ivanti Connect Secure antes da versão 22.7R2.9 ou 22.8R2, no Ivanti Policy Secure antes da versão 22.7R1.6, no Ivanti ZTA Gateway antes da versão 2.8R2.3-723 e no Ivanti Neurons for Secure Access anterior à versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor autenticado remoto sequestre conexões HTML5 existentes. (CVE-2025-55145)
- Um valor de retorno não verificado no Ivanti Connect Secure antes de 22.7R2.9 ou 22.8R2, Ivanti Policy Secure antes de 22.7R1.6, Ivanti ZTA Gateway antes de 2.8R2.3-723 e Ivanti Neurons for Secure Access antes de 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor autenticado remoto com privilégios de administrador acione uma negação de serviço. (CVE-2025-55146)
- O CSRF no Ivanti Connect Secure anterior à versão 22.7R2.9 ou 22.8R2, ao Ivanti Policy Secure anterior à versão 22.7R1.6, ao Ivanti ZTA Gateway anterior à versão 2.8R2.3-723 e ao Ivanti Neurons for Secure Access anterior à versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor remoto não autenticado execute ações confidenciais em nome do usuário vítima. A interação do usuário é necessária.

(CVE-2025-55147)

- SSRF no Ivanti Connect Secure antes de 22.7R2.9 ou 22.8R2, Ivanti Policy Secure antes de 22.7R1.6, Ivanti ZTA Gateway antes de 2.8R2.3-723 e Ivanti Neurons for Secure Access antes de 22.8R1.4 (correção implantada em 02-Aug-2025) permite que um invasor autenticado remoto com privilégios de administrador enumere serviços internos.

(CVE-2025-55139)

- A falta de autorização no Ivanti Connect Secure antes da versão 22.7R2.9 ou 22.8R2, no Ivanti Policy Secure antes da versão 22.7R1.6, no Ivanti ZTA Gateway anterior à versão 2.8R2.3-723 e no Ivanti Neurons for Secure Access anterior à versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor autenticado remotamente com privilégios de administrador somente leitura defina as configurações relacionadas à autenticação. (CVE-2025-55141, CVE-2025-55142)

- A injeção de texto refletida no Ivanti Connect Secure antes da versão 22.7R2.9 ou 22.8R2, no Ivanti Policy Secure antes da versão 22.7R1.6, no Ivanti ZTA Gateway antes da versão 2.8R2.3-723 e no Ivanti Neurons for Secure Access antes da versão 22.8R1.4 (correção implantada em 02 de agosto de 2025) permite que um invasor remoto não autenticado injete texto arbitrário em uma resposta HTTP criada. A interação do usuário é necessária.

(CVE-2025-55143)

A exploração bem-sucedida da mais grave dessas vulnerabilidades pode permitir a execução remota de código no contexto do sistema. Dependendo dos privilégios associados ao sistema, um invasor pode instalar programas; Visualize, altere ou exclua dados.