Várias vulnerabilidades descobertas em Ivanti Connect Secure, Policy Sec

Data: 2025-09-09 17:30:59

Autor: Inteligência Against Invaders

Ivanti, em 9 de setembro, lançou um consultivo de segurança Média e Mediumfive HighSeverity Vulneritities impactando Ivanti Connect SecurePolicy Secure, ZTA Gateways e neurônios para acesso seguro.

Nenhuma evidência de exploração de clientes surgiu até agora. Patches e correções estão disponíveis imediatamente para abordar questões que variam de verificações de autorização ausentes e falsificação de solicitação de sites cruzados (CSRF) falhas nas condições de falsificação de solicitação do lado do servidor (SSRF) e negação de serviço.

Escopo de vulnerabilidades

O consultivo abrange vários componentes, incluindo produtos locais e em nuvem.

As versões afetadas incluem Ivanti Connect Secure 22.7R2.8 e anterior, Política Segura 22.7R1.4 e anterior, ZTA Gateways 22.8R2.2 e neurônios para acesso seguro 22.8R1.3 e anterior.

Ivanti implantou correções em 2 de agosto de 2025, para todos os produtos; Os ambientes de nuvem para neurônios para acesso seguro foram atualizados automaticamente.

Número cve	Descrição	Pontuação do CVSS	Gravidade
CVE-2025-8712	A autorização ausente permite que o administrador somente leitura autenticado remoto altere as configurações restritas.	5.4	Médio
CVE-2025-8711	O CSRF permite que o atacante não autenticado remoto realize ações limitadas com a interação da vítima.	5.4	Médio
CVE-2025-55145	A autorização ausente permite que o invasor autenticado remoto sequestre conexões HTML5 existentes.	8.9	Alto
CVE-2025-55146	O valor de retorno	4.9	Médio

Número cve	Descrição	Pontuação do CVSS	Gravidade
	desmarcado permite que o administrador autenticado remoto acione a negação de serviço.		
CVE-2025-55147	O CSRF permite que o invasor não autenticado remoto execute ações confidenciais com a interação do usuário.	8.8	Alto
CVE-2025-55148	A autorização ausente permite que o administrador somente leitura autenticado remoto configure configurações restritas.	7.6	Alto
CVE-2025-55139	O SSRF permite que o administrador autenticado remoto enumerar os serviços internos.	6.8	Médio
CVE-2025-55141	A autorização ausente permite que o administrador somente leitura autenticado remoto configure a autenticação.	8.8	Alto
CVE-2025-55142	A autorização ausente permite que o administrador somente leitura autenticado remoto configure a autenticação.	8.8	Alto
CVE-2025-55143	A injeção de texto refletida permite que o invasor não autenticado remoto injete a resposta arbitrária de HTTP.	6.1	Médio
CVE-2025-55144	A autorização ausente permite que o Remote autenticado somente leitura admin para definir configurações restritas.	5.4	Médio

Mitigação e recomendações

Implantação de patches:

- Ivanti Connect Seguro: Atualização para 22.7R2.9 ou 22.8R2 através do portal de download

Ivanti.

- Política Ivanti Segura: Atualize para 22.7R1.5 a partir do portal.
- Gateways ZTA: Download da versão 22.8R2.3-723 na interface do controlador.
- Neurônios para acesso seguro: nenhuma ação do cliente é necessária; FIXE a aplicada automaticamente em nuvem em 2 de agosto.

Os clientes devem evitar expor portais administrativos diretamente à Internet. Restringir o acesso por meio de controles de rede alinham -se às orientações de segurança da Ivanti e às melhores práticas do setor.

Ivanti Obrigado, o pesquisador de segurança Nikolay Semov por relatar CVE-2025-55145. Para detalhes sobre a política de divulgação de vulnerabilidades da Ivanti, visite a página de suporte Ivanti.

Garantir que os componentes de software estejam atualizados é crítico. Os administradores devem aplicar esses patches imediatamente para manter a integridade e a segurança do acesso remoto e das implantações de gateway de trust zero.

Encontre esta história interessante! Siga -nosLinkedIneXPara 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.