CISA Problem Alert sobre a exploração ativa da falha de escalada do Micro

Data: 2025-10-07 08:23:11

Autor: Inteligência Against Invaders

A Agência de Segurança de Segurança Cibernética e Infraestrutura dos EUA (CISA) alertou para a

exploração ativa de uma vulnerabilidade crítica de escalada de privilégios no Microsoft Windows.

Conhecido como CVE-2021-43226essa falha reside no driver Common Log File System (CLFS). Os invasores que obtêm acesso local podem ignorar os controles de segurança e elevar seus privilégios, potencialmente levando a um compromisso completo do sistema.

Antecedentes da vulnerabilidade

O driver CLFS é um componente principal do Windows, responsável pelo gerenciamento de arquivos de log que rastreiam os eventos do sistema e do aplicativo.

O CVE-2021-43226 foi divulgado pela Microsoft pela primeira vez no final de 2021, mas a inteligência recente indica que os atores de ameaças começaram a alavancar a falha nas campanhas de ransomware.

Produto	Cve	Descrição
Windows	CVE-2021-43226	Microsoft Windows Common Log File System Driver contém uma vulnerabilidade de escalada de privilégio, permitindo o desvio dos controles

Embora ainda não esteja claro quais grupos específicos estão explorando a vulnerabilidade, o súbito aumento nos incidentes relacionados levou a CISA a adicionar esse problema ao seu conhecido catálogo de vulnerabilidades exploradas em 6 de outubro de 2025.

As vulnerabilidades de escalada de privilégios locais representam um risco sério, porque permitem que os invasores obtenham níveis mais altos de acesso do que o originalmente permitido.

Em ataques direcionados, os adversários costumam encadear tais falhas com vulnerabilidades de execução de código remoto.

Pela primeira vez executando o código através de um serviço exposto ou ataque de phishingeles então usam CVE-2021-43226 para se mover lateralmente dentro de uma rede e acessar dados sensíveis.

Qualquer organização executando versões afetadas do Microsoft Windows está em risco se os atacantes locais puderem acessar um sistema.

Estações de trabalho e servidores que host Dados sensíveis, aplicativos críticos ou ferramentas de gerenciamento de nuvem são alvos principais.

A vulnerabilidade não requer interação do usuário além do invasor que executa o código com privilégios básicos.

Como resultado, as equipes de segurança devem agir rapidamente para evitar escalações de privilégios não autorizadas que possam levar a roubo de dadoscriptografia para resgate ou sabotagem de fluxos de trabalho críticos.

As organizações pequenas e de médio porte podem enfrentar desafios específicos, pois geralmente não têm equipes dedicadas de resposta a incidentes ou extensos processos de gerenciamento de patches.

Sem mitigação oportuna, mesmo uma única estação de trabalho comprometida pode permitir que um invasor obtenha acesso ao administrador do domínio, dando a eles controle sobre uma rede inteira.

CISA Recomenda que todos os usuários afetados apliquem mitigações fornecidas pela Microsoft sem demora. Isso inclui a instalação das atualizações de segurança mais recentes e a garantia de que as ferramentas de proteção de terminais detectem e bloqueem tentativas conhecidas de exploração.

As organizações que usam serviços em nuvem devem seguir a orientação na diretiva operacional vinculativa (BOD) 22-01, que exige divulgações de vulnerabilidades coordenadas e gerenciamento de patches para agências e contratados federais.

Onde as atualizações imediatas não são viáveis, os proprietários de sistemas devem considerar solucionamentos alternativos temporários, como restringir o acesso ao driver CLFS ou isolar sistemas de alto risco.

A interrupção do uso de instalações do Windows não suportadas ou não gerenciadas reduzirá a exposição. As equipes de segurança também devem revisar os registros para obter a atividade incomum do driver CLFS e configurar alertas para eventos que podem indicar tentativas de exploração.

Ao abordar o CVE-2021-43226 por meio de adesivos, monitoramento e conformidade de orientação imediatos, as organizações podem mitigar o risco de escalações de privilégios e proteger ativos críticos do ransomware e outras ameaças cibernéticas.

Siga -nosGoogle NewsAssim,LinkedIneXPara obter atualizações instantâneas e definir GBH como uma fonte preferida em Google.