A vulnerabilidade da ferramenta NVidia NVDebug permite que os invasores

Data: 2025-09-11 09:16:16

Autor: Inteligência Against Invaders

Uma vulnerabilidade crítica na ferramenta NVDebug da NVIDIA pode permitir que os invasores

obtenham acesso elevado ao sistema, execute código ou adulteração com dados.

A NVIDIA lançou um boletim de segurança em 8 de setembro de 2025, relatando três falhas distintas na ferramenta NVDebug e instando todos os usuários a atualizar para a versão 1.7.0 ou posterior.

A falha na atualização pode expor os sistemas a Escalada de privilégiosnegação de serviço e divulgação de informações sensíveis.

Natureza das vulnerabilidades

A atualização de segurança aborda três falhas de alta severidade no utilitário NVDebug. A primeira falha (CVE-2025-23342) pode permitir que um usuário com direitos limitados para executar o código em um nível de privilégio mais alto.

Cve id	Descrição	Pontuação base	Gravidade
CVE-2025-23342	Escalada de privilégios via ferramenta NVDebug, levando à execução de código e violação de dados	8.2	Alto
CVE-2025-23343	Vulnerabilidade de gravação de arquivo, permitindo adulteração de componentes restritos	7.6	Alto
CVE-2025-23344	Execução de código no host como usuário não privilegiado com escalada de privilégio	7.3	Alto

Ao explorar este bug, um atacante poderia correr comandos arbitrárioscausar uma condição de negação de serviço ou obtenha acesso a dados que devem ser protegidos.

A segunda falha (CVE-2025-23343) permite escrever arquivos em locais restritos, levando potencialmente a vazamentos de informações e componentes do sistema corrompido.

A terceira falha (CVE-2025-23344) permite a execução do código no host como um usuário não privilegiado, mas ainda permite a escalada de privilégios e adulteração de dados.

Todas as três vulnerabilidades compartilham um risco comum: se um invasor as acertar com sucesso ou direcionar vários sistemas, eles poderão assumir o controle total das máquinas afetadas ou interromper as operações.

Nvidia Tabiliza cada falha Ashighseverity, com pontuações de base variando de 7,3 a 8,2 na escala CVSS v3.1.

Versões afetadas e instruções de atualização

As falhas afetam todas as versões da ferramenta NVDEBUG antes de 1.7.0 nos sistemas x86_64 e Arm64-SBSA.

Para proteger contra essas vulnerabilidades, a NVIDIA recomenda fortemente o download e a instalação de NVDebug versão 1.7.0 ou posterior no repositório de ferramentas de desenvolvedor da NVIDIA.

Além de atualizar, as organizações devem manter as melhores práticas para o gerenciamento de vulnerabilidades. A inscrição regularmente aos Boletins de Segurança da NVIDIA garante alertas oportunos para questões futuras.

Monitorando os logs do sistema para atividades incomuns e restringir o acesso às ferramentas de desenvolvedor podem reduzir a superfície de ataque.

Se alguma anomalias aparecer após a atualização, entre em contato com a segurança do produto da NVIDIA ou relate possíveis problemas por meio de sua página de segurança.

Manter -se atualizado com atualizações de segurança e implementação de defesas em camadas ajudará a proteger os sistemas contra ameaças emergentes.

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