(/)

Recomendação 10/2026 do CTIR Gov - Atualização

Recomendação Técnica – Vulnerabilidades CVE-2025-4527 e CVE-2025-4528 em Sistemas Dígitro – Atualização

https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2026/recomendacao-10-2026 (https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2026/recomendacao-10-2026)

Publicado em 12/09/2025 11h59 Atualizado em 21/05/2026 14h54

1. O CTIR Gov, em conjunto com informações fornecidas pela fabricante Dígitro Tecnologia S.A., esclarece e atualiza as recomendações anteriores (05/2026 e 09/2026) referentes a vulnerabilidades ativas em software da empresa. As vulnerabilidades identificadas pelos códigos CVE-2025-4526, CVE-2025-4527 e CVE-2025-4528 foram corrigidas pela fabricante nas versões mais recentes do produto NGC Explorer.

1.1. Produtos afetados:
Exclusivamente o NGC Explorer em versões iguais ou inferiores à 3.48.21. Os produtos UNA e GUARDIÃO não são afetados por essas vulnerabilidades.

1.2. Correção disponível:
A versão NGC Explorer 3.48.22 (ou superiores) contém todos os patches de segurança, incluindo:
– Reforço dos mecanismos de controle e invalidação de sessão (CVE-2025-4528);
– Aprimoramento das validações de segurança no lado servidor e dos mecanismos de autenticação (CVE-2025-4527);
– Revisão de controles relacionados à exposição de informações do usuário na interface de configuração (CVE-2025-4526).

2. Características das vulnerabilidades corrigidas:
– CVE-2025-4526: Exposição de informação do usuário na interface de configuração, podendo impactar a confidencialidade de credenciais em cenários específicos de acesso administrativo.
– CVE-2025-4527: Validação de segurança realizada parcialmente no lado cliente, com potencial de bypass em condições específicas, dependendo de exploração complexa.
– CVE-2025-4528: Controle insuficiente de expiração de sessão, podendo permitir reutilização indevida de sessões em cenários específicos.

3. Ações obrigatórias para mitigação e proteção da infraestrutura:

3.1 Atualização imediata do software
– Atualizar o NGC Explorer para a versão 3.48.22 ou superior, disponível exclusivamente no site oficial da Dígitro Tecnologia S.A.

– Antes de aplicar qualquer atualização, validar a integridade dos arquivos junto a representantes oficiais da fabricante (contato oficial da Dígitro).

3.2 Restrição de acesso e segregação de rede (medida permanente)
– Bloquear todo acesso externo/remoto a interfaces administrativas de equipamentos Dígitro (incluindo NGC Explorer, UNA e Guardião, mesmo não afetados).
– Interfaces de gerenciamento não devem ser expostas à internet ou a redes não segregadas.
– Configurações, manutenções ou auditorias devem ser realizadas preferencialmente via acesso físico/direto ao equipamento (console local) ou, quando estritamente necessário, via VPN com controle de acesso rigoroso.

3.3 Monitoramento de rede e regras de firewall
– Monitorar comunicações anômalas originadas ou destinadas a equipamentos Dígitro. Qualquer tráfego não identificado como essencial deve ser tratado como suspeito de exfiltração.
– Implementar no firewall o bloqueio de protocolos de administração remota (SSH, RDP, HTTP/HTTPS administrativo, etc.) apontados para a infraestrutura dos sistemas Guardião, UNA ou NGC Explorer a partir de redes externas não confiáveis.

4. Recomendações adicionais de boas práticas (já integrantes das orientações regulares da Dígitro):
– Restrição à exposição de interfaces administrativas;
– Segregação de rede (redes administrativas separadas de redes de usuários e internet);
– Monitoramento contínuo de logs e tentativas de acesso;
– Validação de integridade de atualizações junto à fabricante.

5. Comunicação de incidentes: Caso seja identificada qualquer comunicação anômala, tentativa de acesso não autorizado ou suspeita de comprometimento de credenciais vinculadas a sistemas Dígitro (mesmo após a atualização), o órgão deve reportar imediatamente ao CTIR Gov pelo e-mail ctir@ctir.gov.br.

[TLP:CLEAR]

Categoria
Comunicações e Transparência Pública

Assine nossas newsletters

Conteúdo estratégico direto no seu e-mail.

Sobre Nós

Sobre nós

Trabalhe conosco

Relatório de Transparência Salarial

Termo de Uso de dados pessoais

Segurança da informação

Lei Geral de Proteção de Dados Pessoais

Compliance Dígitro

Hub de Conhecimento

Fale Conosco

Entre em contato

Onde Estamos

Soluções

Atendimento e Comunicação para Empresas

Atendimento e Comunicação para Administração Pública

Inteligência e Investigação para Segurança Pública e Defesa

Mapa do Site (https://digitro.com/mapa-do-site/)

Serviços

Desenvolvimento de Bots para Atendimento ao Cliente

Noc

Analytics – Business Intelligence

Segmentos

Cidades Inteligentes

Cidades Inteligentes Utilities

Comércio: Atacado, Varejo e Serviços

Cidades Seguras

Cooperativas de Crédito

Provedores

Saúde

Segurança Pública

APIs Dígitro

Portal de APIs Dígitro

Documentação oficial

Produtos Descontinuados

Explore

Blog

Cases

Sala de imprensa

Capacitação

Conteúdos Digitais

Parceiros de Negócio

Parceiros Dígitro

Localize um Parceiro de Negócio

Suporte Técnico ao Parceiro

Academia Dígitro

Academia

Glossário

Dicas rápidas

Acesse o EAD

Treinamentos

Suporte técnico

Perguntas Frequentes

Formulário de Suporte

Telefone Matriz

(48) 3281-7000
(tel:4832817000)

Atendimento ao Cliente

0300 789 8111
(tel:03007898111)

Associações

Parceiros Estratégicos Dígitro

mtools
(https://lp.mtools.digital/inicio?utm_source=parceiro&utm_medium=botao&utm_campaign=site_digitro)