CISA emite 10 avisos de ICS detalhando vulnerabilidades e explorações - A

Data: 2025-08-08 09:55:20

Autor: Inteligência Against Invaders

Inteligência Against Invaders

2025-08-08 06:47

A Agência de Segurança Cibernética e Infraestrutura (CISA) divulgou dez avisos de sistemas de controle industrial (ICS) em 7 de agosto de 2025, destacando vulnerabilidades críticas em várias plataformas de automação e controle industrial.

Esses avisos representam um esforço abrangente para abordar as lacunas de segurança que podem afetar as operações de infraestrutura crítica em vários setores, incluindo sistemas de manufatura, energia e transporte.

CISA O último lote de avisos de sistemas de controle industrial demonstra o compromisso contínuo da agência em proteger a infraestrutura crítica contra ameaças de segurança cibernética em evolução.

Os dez avisos abordam coletivamente vulnerabilidades que abrangem diferentes fornecedores e plataformas de sistemas de controle industrial, cada um apresentando desafios de segurança exclusivos que exigem atenção imediata de operadores industriais e profissionais de segurança cibernética.

1. Delta Electronics DIAView (ICSA-25-219-01)

Uma falha de passagem de caminho (CWE-22) no DIAView v4.2.0.0 e anteriores permite que invasores remotos leiam ou gravem arquivos arbitrários.

- CVE-2025-53417: CVSS v3.1 9.8; CVSS v4.0 9.3

2. Johnson controla FX80 e FX90 (ICSA-25-219-02)

Uma dependência de um componente de terceiros vulnerável (CWE-1395) permite o comprometimento da configuração.

- CVE-2025-43867: CVSS v3.1 7.7; CVSS v4.0 8.4

3. Tecnologia Burk ARC Solo (ICSA-25-219-03)

A autenticação ausente para função crítica (CWE-306) em versões anteriores à v1.0.62 permite o controle por meio do endpoint de alteração de senha.

- CVE-2025-5095: CVSS v3 9.8; CVSS v4 9.3

4. Arena de Automação Rockwell (ICSA-25-219-04)

Várias vulnerabilidades de execução de código local devido a estouros de buffer de leitura, baseados em pilha e heap fora dos limites.

- CVE-2025-7025, CVE-2025-7032, CVE-2025-7033: CVSS v3.1 7.8; CVSS v4.0 8.4

5. Potência do pacote EMX e EG (ICSA-25-219-05)

Autenticação ausente para função crítica (CWE-306) na interface da Web padrão.

- CVE-2025-8284: CVSS v3.1 9.8; CVSS v4.0 9.3

6. Aplicativos móveis Dreame Technology iOS e Android (ICSA-25-219-06)

A validação de certificado inadequada (CWE-295) permite ataques man-in-the-middle em conexões TLS autoassinadas.

- CVE-2025-8393: CVSS v3.1 7.3; CVSS v4.0 8.5

7. Inversores EG4 Electronics EG4 (ICSA-25-219-07)

Transmissão de texto não criptografado, desvio de integridade de firmware, divulgação de informações por meio de discrepância observável e tentativas excessivas de autenticação.

- CVE-2025-52586: CVSS v3.1 6.9; CVSS v4.0 7.5
- CVE-2025-53520: CVSS v3.1 8.8; CVSS v4.0 8.6
- CVE-2025-47872: CVSS v3.1 5.8; CVSS v4.0 6.9
- CVE-2025-46414: CVSS v3.1 8.1; CVSS v4.0 9.2

8. Telefones IP Yealink & RPS (ICSA-25-219-08)

Várias falhas — tentativas excessivas de autenticação (CWE-307), falta de limitação de taxa (CWE-770), autorização incorreta (CWE-863) e validação de certificado inadequada (CWE-295).

- CVE-2025-52916: CVSS v3 2.2; CVSS v4 2.1
- CVE-2025-52917: CVSS v3 4.3; CVSS v4 5.3
- CVE-2025-52918: CVSS v3 5.0; CVSS v4 5.3
- CVE-2025-52919: CVSS v3 4.3; CVSS v4 5.3

9. Instantâneo Micromate (ICSA-25-148-04)

Autenticação ausente para função crítica (CWE-306) na porta de configuração quando conectada via modem.

- CVE-2025-1907: CVSS v3.1 9.8; CVSS v4.0 9.3

10. Mitsubishi Electric ICONICS e Mitsubishi Electric Products (ICSA-25-140-04)

Execução com privilégios desnecessários (CWE-250) via link simbólico no agente AlarmWorX64 Pager.

- CVE-2025-0921: CVSS v3.1 6.5; CVSS v4.0 8.3
- CVE-2025-7376: CVSS v3.1 5.9; CVSS v4.0 4.1

O lançamento de dez avisos de sistemas de controle industrial da CISA ressalta a natureza persistente e evolutiva de Ameaças à segurança cibernética enfrentando infraestrutura crítica.

As organizações que operam sistemas de controle industrial devem permanecer vigilantes na implementação de programas abrangentes de segurança cibernética que abordem vulnerabilidades conhecidas e vetores de ameaças emergentes.

A colaboração contínua entre agências governamentais, fornecedores e operadoras continua sendo essencial para manter a segurança e a resiliência dos sistemas de infraestrutura crítica que sustentam a sociedade moderna.