
aptel
snt
XXII 2026

Framework de Cibersegurança para Videomonitoramento IP: Detecção de Vulnerabilidades, Análise de Riscos e Apoio à Seleção de Sistemas

Glauber Nascimento

Analista Sênior de Segurança da Informação
Engenheiro de Telecomunicações pelo CEFET-RJ

Rodrigo Mello (Orientador)

Professor PhD Eng. de Telecom do CEFET-RJ
Especialista em Cibersegurança e Cientista de Dados

CEFET/RJ



1. INTRODUÇÃO E MOTIVAÇÃO

- Videomonitoramento IP
- Aumento do número de câmeras
  - Mais de 1 Bilhão em 2026. Cerca de 700 Milhões em 2019
- Um dos principais alvos dos atacantes
  - Alto poder computacional
  - Conexão constante com a rede
  - Uso de credenciais pouco complexas







2. OBJETIVOS E CONTRIBUIÇÃO

- Propor um framework abrangente para detecção de vulnerabilidades no ambiente de videomonitoramento IP
  - Através de uma gama de testes de segurança
- Avaliar os riscos associados através de um score unificado
  - Considerando severidade técnica, impacto potencial e probabilidade de exploração
- Definir critérios para comparar, selecionar e homologar soluções de videomonitoramento
  - Auxiliando em processos de aquisição e contratação



3. SELEÇÃO DOS TESTES

TIPO

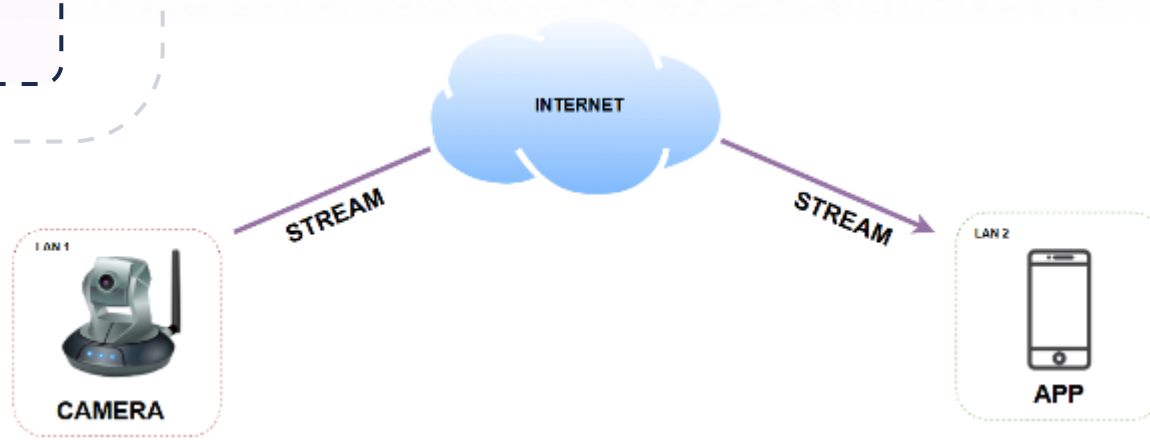
- Câmera
- Aplicação
- Streaming

DIMENSÕES DE RISCO

- Acesso indevido ao streaming
- Indisponibilidade do sistema
- Aumento da superfície de ataque

INDICADORES TÉCNICOS

- Severidade técnica (CVSS)
- Probabilidade de exploração (EPSS)



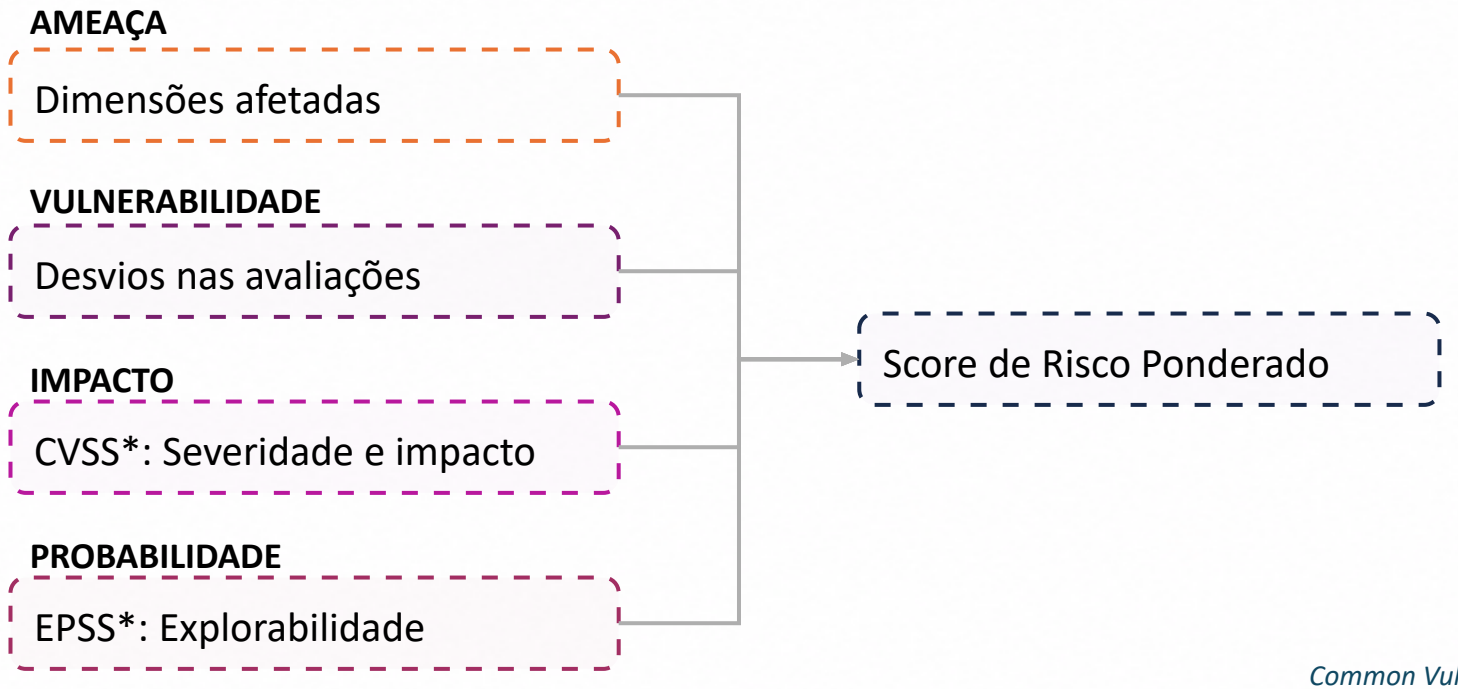
4. CADERNO DOS TESTES BASE

Definição do teste					
ID	**Tipo**	**Cenário**	**Procedimento**	**Avaliação**	**Resultado seguro**
C1	**Câmera**	Atualização de firmware	Análise do aplicativo de gerenciamento	O fabricante fornece atualizações de forma recorrente? S/N	Sim
C2	**Câmera**	Segurança física da câmera	Inspeção do corpo da câmera	A câmera expõe informações sensíveis em seu corpo, como senhas ou QR Codes? S/N	Não
C3	**Câmera**	Portas de comunicação abertas	Varredura de portas	As portas de comunicação estão expostas de forma inadequada? S/N	Não
C4	**Câmera**	Negação de serviço	Emulação de DoS	O sistema é resiliente a ataques de DoS? S/N	Sim
C5	**Câmera**	Interação com ONVIF	Teste de requisições não autenticadas	O ONVIF permite interações não autenticadas? S/N	Não
A1	**Aplicativo**	Comunicação em texto claro	Análise do AndroidManifest.xml	O aplicativo transmite dados em texto claro? S/N	Não
A2	**Aplicativo**	Permissões perigosas ou desnecessárias	Análise do AndroidManifest.xml	O aplicativo solicita permissões além de seu escopo essencial? S/N	Não
A3	**Aplicativo**	Métodos de autenticação	Análise dos métodos de autenticação e gerenciamento de contas	Os métodos de autenticação são frágeis ou estão configurados de forma inadequada? S/N	Não
A4	**Aplicativo**	Vulnerabilidades no código	Análise estática do aplicativo	O aplicativo contém vulnerabilidades de código de alta severidade? S/N	Não
S1	**Streaming**	Criptografia do streaming	Análise de pacotes	A transmissão de dados é protegida por TLS? S/N	Sim
S2	**Streaming**	Descoberta da URL RTSP	Teste de descoberta de URL RTSP	A URL RTSP pode ser descoberta por tentativa automatizada? S/N	Não



5. COMPOSIÇÃO DO SCORE DE RISCO

- Risco: composto por uma combinação de **ameaça, vulnerabilidade, impacto e probabilidade**



Common Vulnerability Scoring System (CVSS)

Exploit Prediction Scoring System (EPSS)

6. CADERNO DE TESTES EXPANDIDO

Definição		Dimensões				Severidade técnica (CVSS)		Probabilidade de exploração (EPSS)	
ID	Cenário	A	I	S	Dimensões	CVSS	Severidade	CVEs associados	P.E.E
C1	Atualização de firmware	☐	☐	☐	**3**	**9,8**	Crítica	CVE-2023-5747; CVE-2023-23120; CVE-2020-27540	**0,00553**
C2	Segurança física da câmera	☐	☐	☐	**3**	**6,8**	Média	CVE-2018-12668; CVE-2016-2358; CVE-2026-58453	**0,01881**
C3	Portas de comunicação abertas	☐	☐	☐	**3**	**9,8**	Crítica	CVE-2025-7503; CVE-2021-4469	**0,00607**
C4	Negação de serviço		☐	☐	**2**	**7,5**	Alta	CVE-2013-4977; CVE-2018-6407; CVE-2019-6973; CVE-2010-4234	**0,16431**
C5	Interação com ONVIF	☐	☐	☐	**3**	**9,8**	Crítica	CVE-2025-65856; CVE-2025-64770; CVE-2018-20051	**0,0078**
A1	Comunicação em texto claro	☐		☐	**2**	**6,5**	Média	CVE-2025-59406; CVE-2025-59405; CVE-2024-25731	**0,0038**
A2	Permissões perigosas ou desnecessárias		☐	☐	**2**	**7,1**	Alta	CVE-2019-2234; CVE-2016-3916; CVE-2016-3834	**0,00465**
A3	Métodos de autenticação	☐	☐	☐	**3**	**9,8**	Crítica	CVE-2025-59403	**0,01067**
A4	Vulnerabilidades no código			☐	**1**	**6,3**	Média	CVE-2025-59407; CVE-2024-13894	**0,00445**
S1	Criptografia do streaming	☐		☐	**2**	**6,5**	Média	CVE-2022-30563	**0,00976**
S2	Descoberta da URL RTSP	☐		☐	**2**	**7,5**	Alta	CVE-2025-66049; CVE-2025-9983; CVE-2026-26340; CVE-2022-45045	**0,00789**



7. SRP DE CADA TESTE

$$SRP = 0,3 \cdot \left(\frac{DR}{3} \times 10\right) + 0,5 \cdot (SB) + 0,2 \cdot (PEE \times 10)$$

SRP: Score de Risco Ponderado

DR: Dimensões de Risco Afetadas; SB: Severidade Base; PEE: Probabilidade de Exploração Estimada

SRP	Risco
0,0	Nenhum
0,1 – 3,9	Baixo
4,0 – 6,9	Médio
7,0 – 8,9	Alto
9,0 – 10,0	Crítico

Definição		Riscos associados				Severidade	Probabilidade de Exploração	Score de risco
ID	Cenário	A	I	S	D.R	S.B	P.E.E	S.R.P
C1	Atualização de firmware	✓	✓	✓	3	9,8	0,00553	7,91
C2	Segurança física da câmera	✓	✓	✓	3	6,8	0,01881	6,44
C3	Portas de comunicação abertas	✓	✓	✓	3	9,8	0,00607	7,91
C4	Negação de serviço	—	✓	✓	2	7,5	0,16431	6,08
C5	Interação com ONVIF	✓	✓	✓	3	9,8	0,0078	7,92
A1	Comunicação em texto claro	✓	—	✓	2	6,5	0,0038	5,26
A2	Permissões perigosas ou desnecessárias	—	✓	✓	2	7,1	0,00465	5,56
A3	Métodos de autenticação	✓	✓	✓	3	9,8	0,01067	7,92
A4	Vulnerabilidades no código	—	—	✓	1	6,3	0,00445	4,16
S1	Criptografia do streaming	✓	—	✓	2	6,5	0,00976	5,27
S2	Descoberta da URL RTSP	✓	—	✓	2	7,5	0,00789	5,77

- A classificação final de cada sistema é calculada através do SRP médio dos testes executados



8. APLICAÇÃO DO FRAMEWORK

- Aplicado em 2 modelos de câmeras muito comuns no Brasil
- Foram utilizadas ferramentas de segurança com credibilidade no mercado



- Câmera ICSee ABQ AP IP pareada com o app Android ICSee v7.5.5



- Câmera Yoosee Wi-Fi IP pareada com o app Android Yoosee v6.32.1

- **Análise do App**: Scan do APK com MobSF
- **Scan de Portas:** NMAP e Nessus Pro
- **Inspeção de tráfego:** Wireshark executado no modelo Proxy
- **Interação com API ONVIF:** Scripts Python Customizados
- **Emulação de DoS:** HPing rodando em uma VM Kali Linux
- **Brute-Force no RTSP:** NMAP Script Engine

9. RESULTADOS DO FRAMEWORK

ID	Cenário	Avaliação	Resultado seguro	ICSee	Yoosee	Detalhes	S.R.P
C1	Atualização de firmware	O fabricante fornece atualizações de forma recorrente? S/N	Sim	**Não**	Sim	O firmware da câmera ICSee data de 2023	7,91
C2	Segurança física da câmera	A câmera expõe informações sensíveis em seu corpo, como senhas ou QR Codes? S/N	Não	Não	**Sim**	A câmera Yoosee expõe códigos QR Codes de pareamento	6,44
C3	Portas de comunicação abertas	As portas de comunicação estão expostas de forma inadequada? S/N	Não	**Sim**	**Sim**	A câmera Yoosee mantém o serviço FTP exposto na porta 21	7,91
C4	Negação de serviço	O sistema é resiliente a ataques de DoS? S/N	Sim	**Não**	Sim	A câmera ICSee teve seu funcionamento completamente interrompido	6,08
C5	Interação com ONVIF	O ONVIF permite interações não autenticadas? S/N	Não	**Sim**	Não	**A câmera ICSee permite operações no ONVIF não autenticadas**	7,92
A1	Comunicação em texto claro	O aplicativo transmite dados em texto claro? S/N	Não	**Sim**	**Sim**	Ambos os aplicativos permitem tráfego em texto claro	5,26
A2	Permissões perigosas ou desnecessárias	O aplicativo solicita permissões além de seu escopo essencial? S/N	Não	**Sim**	**Sim**	Ambos os aplicativos solicitam permissões de alto privilégio	5,56
A3	Métodos de autenticação	Os métodos de autenticação são frágeis ou estão configurados de forma inadequada? S/N	Não	**Sim**	Não	**O aplicativo ICSee apresentou uma vulnerabilidade no mecanismo de bloqueio**	7,92
A4	Vulnerabilidades no código	O aplicativo contém vulnerabilidades de código de alta severidade? S/N	Não	**Sim**	**Sim**	Ambos os aplicativos apresentam vulnerabilidades de alta severidade no código	4,16
S1	Criptografia do streaming	A transmissão de dados é protegida por TLS? S/N	Sim	Sim	**Não**	Não foi identificada criptografia na transmissão de vídeo da câmera Yoosee	5,27
S2	Descoberta da URL RTSP	A URL RTSP pode ser descoberta por tentativa automatizada? S/N	Não	**Sim**	Não	A câmera ICSee utiliza uma URL RTSP conhecida e previsível, afetada pela CVE-2022-45045	5,77



10. COMPARAÇÃO ENTRE OS MODELOS



- Câmera ICSee ABQ AP IP pareada com o app Android ICSee v7.5.5

- Falhou em 9 dos 11 testes propostos
- Apresenta falhas graves na interação via API do ONVIF e na URL RTSP

SRP do sistema: 5,32

RISCO MÉDIO



- Câmera Yoosee Wi-Fi IP pareada com o app Android Yoosee v6.32.1

- Falhou em 6 dos 11 testes propostos
- Tem como principal falha a exposição do QR Code de pareamento

SRP do sistema: 3,14

RISCO BAIXO

11. AUTOMATIZAÇÃO DA ANÁLISE



11. AUTOMATIZAÇÃO DA ANÁLISE

1. Cadastro 2. Testes 3. EPSS 4. Resultado 5. Relatório

Resultados dos 11 testes

Para cada cenário, informe se o sistema está Conforme, Não conforme ou se o teste Não foi executado.

Conforme = atende ao resultado seguro esperado. Não conforme = vulnerabilidade identificada. Não executado = segurança não determinada para esse cenário.

Câmera

- C1 — Atualização de firmware
- C2 — Segurança física da câmera
- C3 — Portas de comunicação abertas
- C4 — Negação de serviço
- C5 — Interação com ONVIF



11. AUTOMATIZAÇÃO DA ANÁLISE

Probabilidade de Exploração — EPSS

A plataforma pode trabalhar em dois modos:

- **Valores de referência do estudo:** reproduzem os valores usados no projeto e permitem validar os resultados históricos.
- **EPSS atualizado:** consulta o FIRST e recalcula a PEE dos cenários com base nos valores atuais.

Fonte atualmente utilizada: Valores de referência do estudo

Usar valores do estudo de caso | Atualizar EPSS via FIRST



11. AUTOMATIZAÇÃO DA ANÁLISE

Resultado dos testes

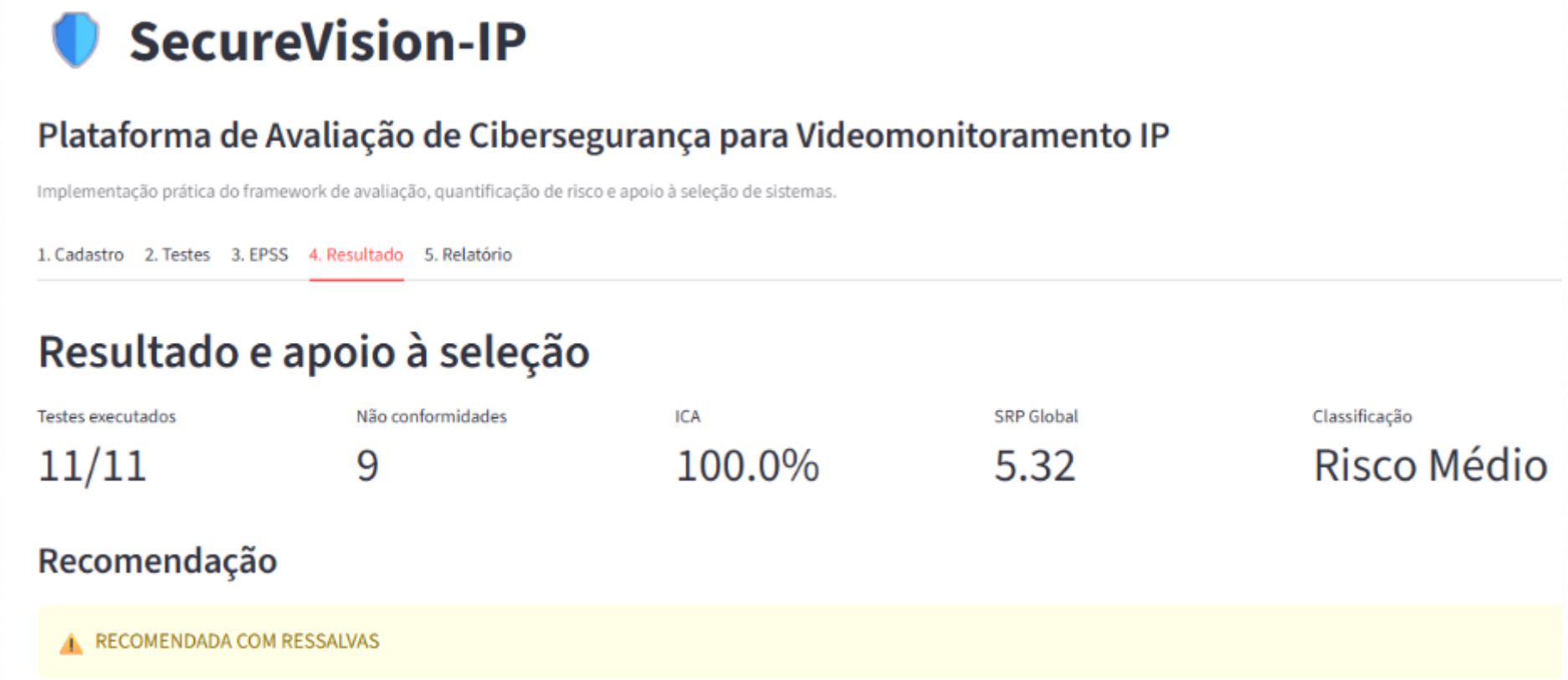
ID	Componente	Teste	Resultado	Resultado seguro	CVSS	Severidade	PEE	SRP Cenário	SRP Atribuído
C1	Câmera	Atualização de firmware	Não conforme	Sim	9.8	Crítica	0.00553	7.91	7.91
C2	Câmera	Segurança física da câmera	Conforme	Não	6.8	Média	0.01881	6.44	0.00
C3	Câmera	Portas de comunicação abertas	Não conforme	Não	9.8	Crítica	0.00607	7.91	7.91
C4	Câmera	Negação de serviço	Não conforme	Sim	7.5	Alta	0.16431	6.08	6.08
C5	Câmera	Interação com ONVIF	Não conforme	Não	9.8	Crítica	0.00780	7.92	7.92
A1	Aplicativo	Comunicação em texto claro	Não conforme	Não	6.5	Média	0.00380	5.26	5.26
A2	Aplicativo	Permissões perigosas ou desnecessárias	Não conforme	Não	7.1	Alta	0.00465	5.56	5.56
A3	Aplicativo	Métodos de autenticação							
A4	Aplicativo	Vulnerabilidades no código							
S1	Streaming	Criptografia do streaming							

Resultado por componente

Componente	SRP	Classificação
Câmera	5.96	Risco Médio
Aplicativo	5.72	Risco Médio
Streaming	2.88	Risco Baixo



11. AUTOMATIZAÇÃO DA ANÁLISE





12. BENEFÍCIOS E CONCLUSÃO

- Torna simples a identificação de vulnerabilidades em sistemas de videomonitoramento
- Permite se antecipar e se proteger contra as principais ameaças aos sistemas de videomonitoramento
- Compara de forma clara diferentes sistemas
- Permite a integração com outras plataformas de gerenciamento de vulnerabilidades
- Metodologia original e inovadora voltada para o mercado



Framework de Cibersegurança para Videomonitoramento IP: Detecção de Vulnerabilidades, Análise de Riscos e Apoio à Seleção de Sistemas

Glauber Nascimento (glauber.nascimento@insi.com)
Analista Sênior de Segurança da Informação
Engenheiro de Telecomunicações pelo CEFET-RJ

Rodrigo Mello (rodrigo.mello@cefet-rj.br)
Professor PhD Eng. de Telecom do CEFET-RJ
Especialista em Cibersegurança e Cientista de Dados

Obrigado!

