MAIO 2026

Penetration Testing Report Details PTBR

Novo Pentest - Host 172.16.10.232 e IPs Publicos

Cliente	**FACIL**
Tipo de teste	Blackbox / validacao de host interno e IPs publicos solicitados
Documento	Relatorio tecnico de Penetration Testing
Preparado por	Microtech
Data	Maio de 2026

Conteudo

1. Aviso Legal

1.1 Isencao de Responsabilidade

Reconhece-se a impossibilidade de testar redes, sistemas, servicos e aplicacoes contra todas as potenciais vulnerabilidades de seguranca. Este relatorio, portanto, nao pode garantir protecao integral dos ativos contra todas as ameacas existentes.

Os testes realizados refletem a perspectiva tecnica da Microtech no periodo de avaliacao e os problemas identificados sao especificos ao contexto, escopo e evidencias disponiveis.

As recomendacoes descritas tem como finalidade apoiar o processo de mitigacao, priorizacao e melhoria da postura de seguranca. A implementacao deve considerar janela de mudanca, impacto operacional, dependencias de terceiros e validacao em ambiente controlado quando aplicavel.

1.2 Declaracao de Confidencialidade

Este documento contem informacoes proprietarias e confidenciais da FACIL e da Microtech. A divulgacao, reproducao, distribuicao ou compartilhamento total ou parcial deve ocorrer somente mediante autorizacao das partes envolvidas.

O conteudo pode conter enderecos de rede, servicos, vulnerabilidades, riscos e recomendacoes que, se divulgados indevidamente, podem ampliar a exposicao do ambiente.

2. Introducao

A Microtech conduziu um novo ciclo de teste de intrusao para a FACIL, direcionado aos hosts solicitados pelo cliente, com o objetivo de avaliar a postura de seguranca dos ativos definidos em escopo, identificar vulnerabilidades tecnicas e apresentar recomendacoes de mitigacao priorizadas por risco.

Este relatorio contempla somente o host interno 172.16.10.232 e os IPs publicos 132.255.223.92, 132.255.223.93 e 132.255.223.94.

Nos IPs publicos avaliados nao foram identificadas vulnerabilidades externas exploraveis no momento da validacao. O comportamento observado indica que a exposicao esta sendo filtrada pelo FortiGate, reduzindo a superficie externa diretamente observavel a partir da internet.

Este relatorio deve ser utilizado como base para planejamento de correcoes, priorizacao de acoes tecnicas, reteste e evolucao continua dos controles de seguranca do ambiente.

3. Sumario Executivo

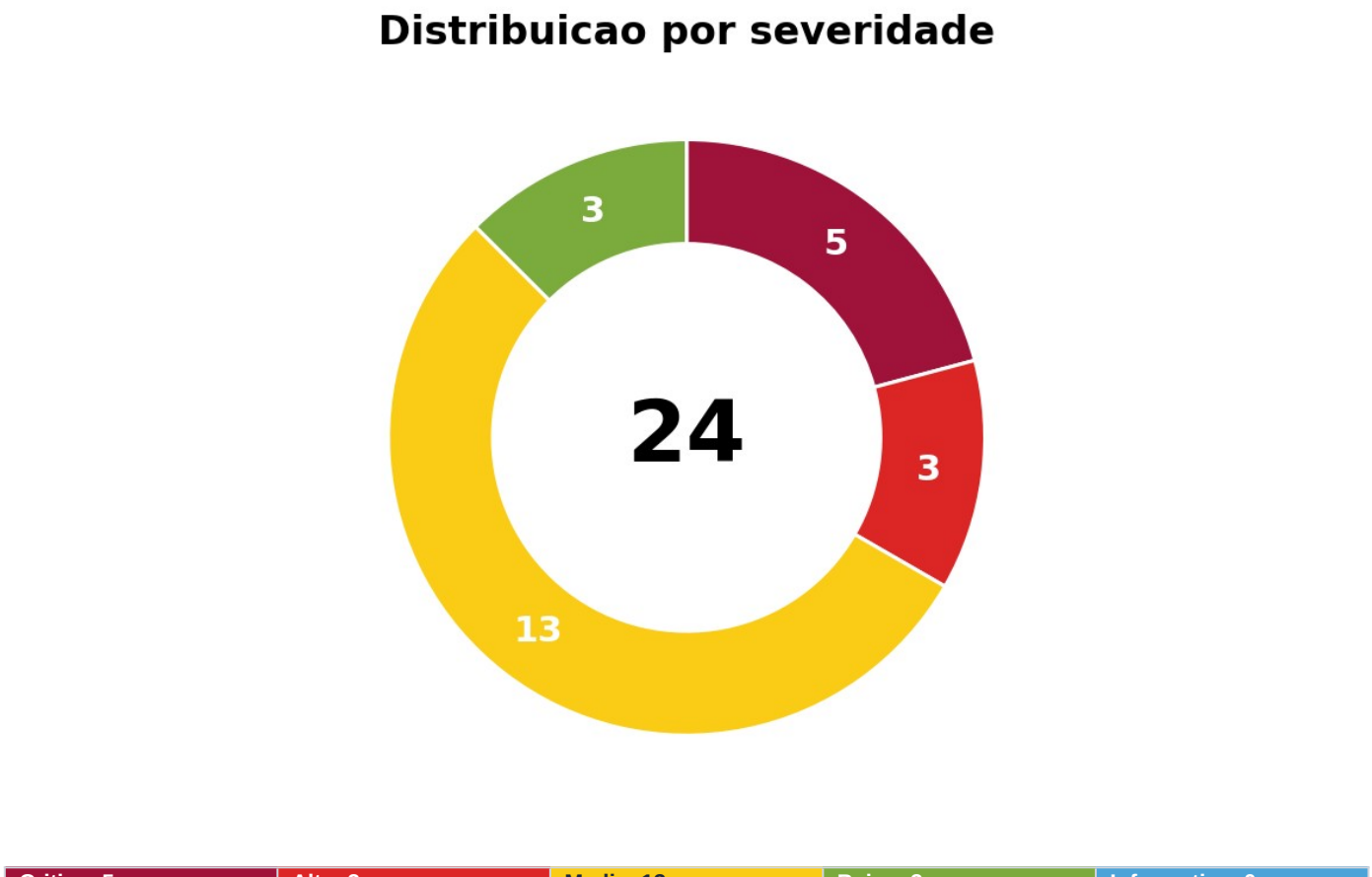
A avaliacao identificou vulnerabilidades relevantes no host interno 172.16.10.232, principalmente relacionadas ao FreePBX, sistema operacional CentOS 7 em fim de vida, exposicao HTTP/HTTPS, componentes desatualizados, metodos HTTP inseguros, parametros TLS/SSL e algoritmos SSH fracos.

Foram consolidadas 24 vulnerabilidades no host 172.16.10.232, classificadas da seguinte forma: 5 criticas, 3 altas, 13 medias, 3 baixas e 0 informativas.

A maior prioridade esta associada as vulnerabilidades classificadas como criticas, principalmente execucao remota de comandos, bypass de autenticacao administrativa no FreePBX e uso de sistema operacional CentOS 7 em fim de vida, que nao recebe atualizacoes regulares de seguranca.

Os IPs publicos 132.255.223.92, 132.255.223.93 e 132.255.223.94 foram incluidos no escopo. Durante a validacao externa, nao foram encontradas vulnerabilidades externas nesses IPs, indicando filtragem pelo FortiGate.

A recomendacao principal e iniciar a mitigacao pelos itens de severidade Critica e Alta, principalmente atualizacao/substituicao do FreePBX, migracao do CentOS 7 para sistema operacional suportado, implantacao de rotina de atualizacao de patches, restricao de acesso aos servicos web, endurecimento de TLS/SSL, revisao de SSH/SMTP e execucao de reteste apos as correcoes.



3.1 Resumo por host

Host	Critica	Alta	Media	Baixa	Total
172.16.10.232	5	3	13	3	24
IPs publicos 132.255.223.92/.93 /.94	0	0	0	0	0

4. Escopo

Campo	Descricao
Ambiente	Producao
Tipo	Blackbox / validacao de host interno e IPs publicos solicitados
Acesso ao codigo fonte	Nao
Host interno	172.16.10.232
Hosts publicos	132.255.223.92; 132.255.223.93; 132.255.223.94
Resultado dos IPs publicos	Sem vulnerabilidades externas identificadas no momento da validacao; trafego filtrado pelo FortiGate.

Fora do Escopo

Nao foram considerados no escopo ataques de engenharia social, phishing contra usuarios, negacao de servico distribuida (DDoS), exploracao destrutiva, alteracao de dados produtivos ou testes que pudessem causar indisponibilidade sem aprovacao previa.

4.1 Metodologia

Reconhecimento e enumeracao
Identificacao de host, portas, protocolos, banners, tecnologias, servicos publicados e caminhos de exposicao externa/interna.

Identificacao de vulnerabilidades
Correlacao de servicos, versoes e componentes com vulnerabilidades conhecidas, fim de vida, ausencia de patches, exposicao de portas e hardening.

Validacao tecnica
Validacao da existencia das vulnerabilidades reportadas, evitando falsas classificacoes sempre que possivel e respeitando limites de seguranca operacional.

Analise de impacto
Avaliacao do potencial impacto para confidencialidade, integridade, disponibilidade, continuidade operacional e exposicao de dados.

Priorizacao
Classificacao por severidade, exposicao, criticidade do ativo, facilidade de exploracao, impacto de negocio e necessidade de correcao.

Relato e recomendacao
Documentacao dos achados com ativos afetados, recomendacoes tecnicas, referencias e criterios de reteste.

A metodologia foi alinhada a praticas reconhecidas como PTES (Penetration Testing Execution Standard), NIST SP 800-115 e uso complementar de referencia CVSS para categorizacao de severidade.

5. Classificacoes de Riscos

A categorizacao de risco utilizada neste relatorio considera a severidade tecnica, a exposicao do ativo, o contexto de negocio e a possibilidade de exploracao. O CVSS e utilizado como referencia geral, complementado por avaliacao contextual do ambiente FACIL.

Severidade	CVSS	Descricao
Critica	9.0 - 10.0	Pode permitir comprometimento direto, amplo ou imediato de sistemas, dados ou operacao. Deve ser tratada imediatamente.
Alta	7.0 - 8.9	Pode permitir comprometimento relevante do ativo ou servico, especialmente quando exposto externamente ou acessivel por redes sensiveis.
Media	4.0 - 6.9	Exige atencao e correcao planejada. Pode ampliar risco quando combinada a outras falhas ou exposicao.
Baixa	0.1 - 3.9	Nao representa risco imediato isolado, mas contribui para enumeracao, exposicao ou fragilidade acumulada.
Informativa	0.0	Nao representa vulnerabilidade direta, mas indica informacao util para melhoria da postura de seguranca.

6. Tabela de Vulnerabilidades

A tabela a seguir apresenta o resumo das vulnerabilidades identificadas no host interno 172.16.10.232 durante o novo ciclo de Pentest.

6.1 Vulnerabilidades - Parte 1

ID	Vulnerabilidade	Severidade	Status	Ativo afetado
PT_FACIL_NP_001	FreePBX vulneravel a execucao remota de comandos via HTTP	Critica	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_002	FreePBX com bypass de autenticacao administrativa via HTTP	Critica	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_003	Sistema operacional CentOS 7 em fim de vida e sem atualizacoes regulares de seguranca	Critica	Nao corrigido	172.16.10.232:sistema operacional
PT_FACIL_NP_004	FreePBX vulneravel a execucao remota de codigo via HTTP	Alta	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_005	FreePBX vulneravel a execucao remota de comandos via HTTPS	Critica	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_006	FreePBX com bypass de autenticacao administrativa via HTTPS	Critica	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_007	FreePBX vulneravel a execucao remota de codigo via HTTPS	Alta	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_008	Cifras SSL/TLS vulneraveis aceitas no servico HTTPS	Alta	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_009	FreePBX com vulnerabilidade de upload arbitrario de arquivo via HTTP	Media	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_010	jQuery desatualizado vulneravel a XSS via HTTP	Media	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_011	Metodo HTTP TRACE habilitado via HTTP	Media	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_012	FreePBX com vulnerabilidade de XSS armazenado via HTTP	Media	Nao corrigido	172.16.10.232:80/tcp

6.2 Vulnerabilidades - Parte 2

ID	Vulnerabilidade	Severidade	Status	Ativo afetado
PT_FACIL_NP_013	Transmissao de informacao sensivel em texto claro via HTTP	Media	Nao corrigido	172.16.10.232:80/tcp
PT_FACIL_NP_014	FreePBX com vulnerabilidade de upload arbitrario de arquivo via HTTPS	Media	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_015	jQuery desatualizado vulneravel a XSS via HTTPS	Media	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_016	Metodo HTTP TRACE habilitado via HTTPS	Media	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_017	FreePBX com vulnerabilidade de XSS armazenado via HTTPS	Media	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_018	Protocolos TLS 1.0 e TLS 1.1 depreciados habilitados	Media	Nao corrigido	172.16.10.232:443/tcp
PT_FACIL_NP_019	Algoritmos fracos de troca de chaves SSH habilitados	Media	Nao corrigido	172.16.10.232:22/tcp
PT_FACIL_NP_020	Algoritmos fracos de criptografia SSH habilitados	Media	Nao corrigido	172.16.10.232:22/tcp
PT_FACIL_NP_021	Servidor SMTP responde a comandos VRFY/EXPN	Media	Nao corrigido	172.16.10.232:25/tcp
PT_FACIL_NP_022	TCP Timestamps permitem inferencia de uptime	Baixa	Nao corrigido	172.16.10.232:general/tcp
PT_FACIL_NP_023	ICMP Timestamp Reply habilitado	Baixa	Nao corrigido	172.16.10.232:general/icmp
PT_FACIL_NP_024	Algoritmos MAC fracos suportados no SSH	Baixa	Nao corrigido	172.16.10.232:22/tcp

6.3 Validacao dos IPs publicos solicitados

Os IPs publicos abaixo foram incluidos no escopo do novo Pentest. Durante a validacao externa, nao foram identificadas vulnerabilidades externas exploraveis nesses enderecos. O comportamento observado indica filtragem pelo FortiGate.

Host/IP	Tipo	Resultado	Observacao tecnica
132.255.223.92	IP publico	Sem vulnerabilidade externa identificada	Trafego filtrado pelo FortiGate no momento da validacao.
132.255.223.93	IP publico	Sem vulnerabilidade externa identificada	Trafego filtrado pelo FortiGate no momento da validacao.
132.255.223.94	IP publico	Sem vulnerabilidade externa identificada	Trafego filtrado pelo FortiGate no momento da validacao.

Observacao: a ausencia de vulnerabilidades externas detectadas no momento do teste nao elimina a necessidade de revisao periodica. Mudancas de NAT, politicas de firewall, servicos publicados ou regras temporarias podem alterar a exposicao futura.

7. Detalhes das Vulnerabilidades

Nas paginas a seguir encontram-se os detalhes das vulnerabilidades identificadas no host interno 172.16.10.232.

PT_FACIL_NP_001 - FreePBX vulneravel a execucao remota de comandos via HTTP

Severidade	CVSS	CWE	Status
Critica	10.0	CWE-78	Nao corrigido

Descricao e impacto

Servico FreePBX com falha que pode permitir execucao remota de comandos no contexto da aplicacao.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar FreePBX e modulos.
- Restringir acesso ao painel/servico por firewall.
- Validar necessidade da exposicao em HTTP/HTTPS.
- Revisar logs, contas e credenciais.
- Executar reteste apos correcao.

PT_FACIL_NP_002 - FreePBX com bypass de autenticacao administrativa via HTTP

Severidade	CVSS	CWE	Status
Critica	9.8	CWE-287	Nao corrigido

Descricao e impacto

Possibilidade de contorno de autenticacao administrativa em servico FreePBX acessivel no host avaliado.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar FreePBX para versao corrigida.
- Bloquear administracao direta fora de redes confiaveis.
- Forcar troca/revisao de senhas administrativas.
- Validar logs de acesso administrativo.

PT_FACIL_NP_003 - Sistema operacional CentOS 7 em fim de vida e sem atualizacoes regulares de seguranca

Severidade	CVSS	CWE	Status
Critica	10.0	CWE-1104	Nao corrigido

Descricao e impacto

O host utiliza CentOS 7, sistema operacional em fim de vida. Sistemas fora de suporte deixam de receber atualizacoes regulares de seguranca, correcoes oficiais e melhorias de estabilidade, elevando o risco de exposicao a vulnerabilidades conhecidas e futuras.

Ativos afetados

172.16.10.232:sistema operacional

Recomendacoes

- Planejar migracao para sistema operacional suportado.
- Validar compatibilidade do FreePBX e dependencias antes da migracao.
- Criar rotina formal de atualizacao de patches para sistema operacional, servicos e aplicacoes.
- Definir janela de manutencao, backup e plano de rollback.
- Executar reteste apos migracao ou mitigacao.

PT_FACIL_NP_004 - FreePBX vulneravel a execucao remota de codigo via HTTP

Severidade	CVSS	CWE	Status
Alta	7.5	CWE-94	Nao corrigido

Descricao e impacto

Falha com potencial de execucao de codigo no servico FreePBX, podendo comprometer a aplicacao e o sistema subjacente.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar aplicacao e dependencias.
- Isolar o servico em rede restrita.
- Aplicar allowlist de origem.
- Realizar varredura e reteste pos-correcao.

PT_FACIL_NP_005 - FreePBX vulneravel a execucao remota de comandos via HTTPS

Severidade	CVSS	CWE	Status
Critica	10.0	CWE-78	Nao corrigido

Descricao e impacto

Servico FreePBX com falha que pode permitir execucao remota de comandos no contexto da aplicacao.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar FreePBX e modulos.
- Restringir acesso ao painel/servico por firewall.
- Validar necessidade da exposicao em HTTP/HTTPS.
- Revisar logs, contas e credenciais.
- Executar reteste apos correcao.

PT_FACIL_NP_006 - FreePBX com bypass de autenticacao administrativa via HTTPS

Severidade	CVSS	CWE	Status
Critica	9.8	CWE-287	Nao corrigido

Descricao e impacto

Possibilidade de contorno de autenticacao administrativa em servico FreePBX acessivel no host avaliado.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar FreePBX para versao corrigida.
- Bloquear administracao direta fora de redes confiaveis.
- Forcar troca/revisao de senhas administrativas.
- Validar logs de acesso administrativo.

PT_FACIL_NP_007 - FreePBX vulneravel a execucao remota de codigo via HTTPS

Severidade	CVSS	CWE	Status
Alta	7.5	CWE-94	Nao corrigido

Descricao e impacto

Falha com potencial de execucao de codigo no servico FreePBX, podendo comprometer a aplicacao e o sistema subjacente.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar aplicacao e dependencias.
- Isolar o servico em rede restrita.
- Aplicar allowlist de origem.
- Realizar varredura e reteste pos-correcao.

PT_FACIL_NP_008 - Cifras SSL/TLS vulneraveis aceitas no servico HTTPS

Severidade	CVSS	CWE	Status
Alta	7.5	CWE-326	Nao corrigido

Descricao e impacto

O servico utiliza protocolos ou cifras depreciadas, reduzindo a postura criptografica e podendo permitir exploracao de falhas conhecidas ou interceptacao em cenarios especificos.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Desabilitar TLS 1.0/TLS 1.1 e cifras fracas.
- Manter TLS 1.2 ou superior com suites fortes.
- Validar compatibilidade dos clientes antes da mudanca.
- Retestar o servico apos ajuste.

PT_FACIL_NP_009 - FreePBX com vulnerabilidade de upload arbitrario de arquivo via HTTP

Severidade	CVSS	CWE	Status
Media	6.5	CWE-434	Nao corrigido

Descricao e impacto

FreePBX apresenta condicao que pode permitir upload de arquivos sem validacao adequada.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar FreePBX.
- Revisar permissoes de diretorios.
- Bloquear upload indevido.
- Validar integridade de arquivos publicados.

PT_FACIL_NP_010 - jQuery desatualizado vulneravel a XSS via HTTP

Severidade	CVSS	CWE	Status
Media	6.1	CWE-79	Nao corrigido

Descricao e impacto

Biblioteca jQuery antiga com vulnerabilidade de XSS, observada nos caminhos web do FreePBX.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar jQuery conforme compatibilidade.
- Validar dependencias do FreePBX.
- Revisar paginas que referenciam biblioteca vulneravel.

PT_FACIL_NP_011 - Metodo HTTP TRACE habilitado via HTTP

Severidade	CVSS	CWE	Status
Media	5.8	CWE-693	Nao corrigido

Descricao e impacto

O metodo HTTP TRACE encontra-se habilitado, podendo contribuir para ataques Cross-Site Tracing quando combinado com outras falhas.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Desabilitar TRACE/TRACK no servidor web.
- Validar configuracao em HTTP e HTTPS.
- Retestar metodos permitidos.

PT_FACIL_NP_012 - FreePBX com vulnerabilidade de XSS armazenado via HTTP

Severidade	CVSS	CWE	Status
Media	4.8	CWE-79	Nao corrigido

Descricao e impacto

FreePBX apresenta vulnerabilidade de Cross-Site Scripting, com risco de execucao de script malicioso em contexto de usuario.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Atualizar FreePBX/modulos.
- Aplicar validacao e sanitizacao.
- Revisar modulos e extensoes de administracao.

PT_FACIL_NP_013 - Transmissao de informacao sensivel em texto claro via HTTP

Severidade	CVSS	CWE	Status
Media	4.8	CWE-319	Nao corrigido

Descricao e impacto

Campos sensiveis foram identificados em HTTP, sem garantia de transmissao protegida por TLS.

Ativos afetados

172.16.10.232:80/tcp

Recomendacoes

- Forcar redirecionamento HTTP para HTTPS.
- Bloquear envio de credenciais via HTTP.
- Revisar formularios e cabecalhos de seguranca.

PT_FACIL_NP_014 - FreePBX com vulnerabilidade de upload arbitrario de arquivo via HTTPS

Severidade	CVSS	CWE	Status
Media	6.5	CWE-434	Nao corrigido

Descricao e impacto

FreePBX apresenta condicao que pode permitir upload de arquivos sem validacao adequada.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar FreePBX.
- Revisar permissoes de diretorios.
- Bloquear upload indevido.
- Validar integridade de arquivos publicados.

PT_FACIL_NP_015 - jQuery desatualizado vulneravel a XSS via HTTPS

Severidade	CVSS	CWE	Status
Media	6.1	CWE-79	Nao corrigido

Descricao e impacto

Biblioteca jQuery antiga com vulnerabilidade de XSS, observada nos caminhos web do FreePBX.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar jQuery conforme compatibilidade.
- Validar dependencias do FreePBX.
- Revisar paginas que referenciam biblioteca vulneravel.

PT_FACIL_NP_016 - Metodo HTTP TRACE habilitado via HTTPS

Severidade	CVSS	CWE	Status
Media	5.8	CWE-693	Nao corrigido

Descricao e impacto

O metodo HTTP TRACE encontra-se habilitado, podendo contribuir para ataques Cross-Site Tracing quando combinado com outras falhas.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Desabilitar TRACE/TRACK no servidor web.
- Validar configuracao em HTTP e HTTPS.
- Retestar metodos permitidos.

PT_FACIL_NP_017 - FreePBX com vulnerabilidade de XSS armazenado via HTTPS

Severidade	CVSS	CWE	Status
Media	4.8	CWE-79	Nao corrigido

Descricao e impacto

FreePBX apresenta vulnerabilidade de Cross-Site Scripting, com risco de execucao de script malicioso em contexto de usuario.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Atualizar FreePBX/modulos.
- Aplicar validacao e sanitizacao.
- Revisar modulos e extensoes de administracao.

PT_FACIL_NP_018 - Protocolos TLS 1.0 e TLS 1.1 depreciados habilitados

Severidade	CVSS	CWE	Status
Media	4.3	CWE-326	Nao corrigido

Descricao e impacto

O servico utiliza protocolos ou cifras depreciadas, reduzindo a postura criptografica e podendo permitir exploracao de falhas conhecidas ou interceptacao em cenarios especificos.

Ativos afetados

172.16.10.232:443/tcp

Recomendacoes

- Desabilitar TLS 1.0/TLS 1.1 e cifras fracas.
- Manter TLS 1.2 ou superior com suites fortes.
- Validar compatibilidade dos clientes antes da mudanca.

- Retestar o servico apos ajuste.

PT_FACIL_NP_019 - Algoritmos fracos de troca de chaves SSH habilitados

Severidade	CVSS	CWE	Status
Media	5.3	CWE-327	Nao corrigido

Descricao e impacto

O servico SSH aceita algoritmos fracos ou depreciados, reduzindo a postura criptografica do acesso remoto.

Ativos afetados

172.16.10.232:22/tcp

Recomendacoes

- Remover algoritmos fracos de KEX, cifras ou MAC.
- Priorizar algoritmos modernos.
- Restringir origem do SSH por firewall.
- Retestar configuracao SSH.

PT_FACIL_NP_020 - Algoritmos fracos de criptografia SSH habilitados

Severidade	CVSS	CWE	Status
Media	4.3	CWE-327	Nao corrigido

Descricao e impacto

O servico SSH aceita algoritmos fracos ou depreciados, reduzindo a postura criptografica do acesso remoto.

Ativos afetados

172.16.10.232:22/tcp

Recomendacoes

- Remover algoritmos fracos de KEX, cifras ou MAC.
- Priorizar algoritmos modernos.
- Restringir origem do SSH por firewall.
- Retestar configuracao SSH.

PT_FACIL_NP_021 - Servidor SMTP responde a comandos VRFY/EXPN

Severidade	CVSS	CWE	Status
Media	5.0	CWE-200	Nao corrigido

Descricao e impacto

Servidor SMTP responde a comandos VRFY/EXPN, permitindo enumeracao parcial de usuarios/enderecos.

Ativos afetados

172.16.10.232:25/tcp

Recomendacoes

- Desabilitar VRFY/EXPN.
- Revisar configuracao do servidor SMTP.
- Validar exposicao SMTP e necessidade operacional.

PT_FACIL_NP_022 - TCP Timestamps permitem inferencia de uptime

Severidade	CVSS	CWE	Status
Baixa	2.6	CWE-200	Nao corrigido

Descricao e impacto

TCP Timestamps permitem inferencia de uptime do sistema e contribuem para enumeracao tecnica.

Ativos afetados

172.16.10.232:general/tcp

Recomendacoes

- Avaliar necessidade de desabilitar timestamps.
- Aplicar mitigacao conforme sistema operacional.
- Tratar como hardening complementar.

PT_FACIL_NP_023 - ICMP Timestamp Reply habilitado

Severidade	CVSS	CWE	Status
Baixa	2.1	CWE-200	Nao corrigido

Descricao e impacto

Host responde a requisicoes ICMP Timestamp, expondo informacao de tempo.

Ativos afetados

172.16.10.232:general/icmp

Recomendacoes

- Bloquear ICMP Timestamp no firewall.
- Manter apenas ICMP necessario para monitoramento.
- Retestar resposta ICMP.

PT_FACIL_NP_024 - Algoritmos MAC fracos suportados no SSH

Severidade	CVSS	CWE	Status
Baixa	2.6	CWE-327	Nao corrigido

Descricao e impacto

O servico SSH aceita algoritmos fracos ou depreciados, reduzindo a postura criptografica do acesso remoto.

Ativos afetados

172.16.10.232:22/tcp

Recomendacoes

- Remover algoritmos fracos de KEX, cifras ou MAC.
- Priorizar algoritmos modernos.
- Restringir origem do SSH por firewall.
- Retestar configuracao SSH.

8. Plano de Correcao e Priorizacao

Prazo	Objetivo	Acoes
Imediato	Reduzir risco critico	Corrigir FreePBX, vulnerabilidades de RCE/auth bypass, restringir origem e avaliar atualizacao/substituicao do servico.
Imediato	Tratar sistema operacional em fim de vida	Planejar migracao do CentOS 7 para sistema operacional suportado, validar dependencias do FreePBX e aplicar patching regular.
Curto prazo	Reduzir exposicao web	Forcar HTTPS, desabilitar HTTP quando possivel, bloquear TRACE e revisar publicacoes 80/443.
Curto prazo	Fortalecer TLS/SSL	Remover 3DES/SWEET32, desabilitar TLS 1.0/1.1 e manter suites modernas em HTTPS.
Curto prazo	Endurecer SSH/SMTP	Remover algoritmos fracos de SSH, restringir origem e revisar comandos VRFY/EXPN no SMTP.
Medio prazo	Gestao de patches	Criar ciclo de atualizacao, inventario de versoes, janela de homologacao, evidencias de aplicacao e verificacao recorrente.
Apos correcoes	Reteste	Executar nova avaliacao para confirmar mitigacao e atualizar status das vulnerabilidades.

9. Criterios de Aceite e Reteste

- Evidencia de atualizacao, correcao ou mitigacao aplicada para cada vulnerabilidade.
- Validacao de que FreePBX e modulos vulneraveis foram atualizados, substituidos ou isolados.
- Evidencia de migracao do CentOS 7 para versao suportada ou aceite formal de risco com plano de prazo definido.
- Comprovacao de rotina de patches para sistema operacional, FreePBX, dependencias e servicos expostos.
- Configuracao TLS revisada com desativacao de protocolos/cifras fracas em HTTPS.
- Configuracao SSH revisada com remocao de KEX, cifras e MACs fracos.
- Restricao de HTTP/HTTPS/SSH/SMTP a origens justificadas e documentadas.
- Registro formal de regra de firewall/NAT, origem permitida e justificativa operacional quando aplicavel.
- Execucao de reteste tecnico para alteracao de status para Corrigido ou Risco Aceito formalmente.

10. Observacao final sobre os IPs publicos

Para os IPs publicos 132.255.223.92, 132.255.223.93 e 132.255.223.94, nao foram encontradas vulnerabilidades externas no momento da validacao. A analise indica que os acessos estao sendo filtrados pelo FortiGate.

A recomendacao e manter a revisao periodica das politicas do FortiGate, principalmente apos qualquer alteracao de NAT, publicacao, rota, VIP, servico liberado ou regra temporaria. A ausencia de achados em uma janela de teste nao substitui monitoramento continuo e governanca de mudancas.