Your Business
August 28, 2026 · 09:06 AM

SECURITY REPORT

4
/10
MEDIUM

SCAN TARGET

cinteltelecom.com

Open ports detected: **0** · Public IP: **108.179.252.18**

A risk score of 4/10 (MEDIUM) indicates your business has security issues that need attention. The higher the score, the greater the chance of a breach, ransomware, or data theft.

EXECUTIVE SUMMARY

The security scan of cinteltelecom.com found 17 issues including 2 high-risk and 5 medium-risk findings. The most critical issue is 'cPanel Exposed' which requires immediate attention. Full remediation steps are provided for each finding below.

✓ Your server is reachable, which means the web checks and SSL analysis were able to run successfully.

TOP RECOMMENDATIONS

1. cPanel Exposed: Restrict access to /cpanel/ by IP allowlist, move it to a non-standard path, or disable it if not needed.
2. Missing DMARC Record — Email Impersonation Risk: Add a DMARC TXT record to your DNS.
3. HTTP Not Redirecting to HTTPS: Add a permanent redirect from HTTP to HTTPS.

DETAILED FINDINGS

cPanel Exposed

Port HTTPS · cPanel Exposed

HIGH

WHAT IT IS	The path /cpanel/ is accessible without authentication — this exposes administration functionality to anyone on the internet
BUSINESS RISK	Publicly reachable admin panels are a primary target for automated attacks. An attacker who can reach /cpanel/ can attempt brute-force login, exploit known vulnerabilities in the admin software, or leverage it as a stepping stone to full server compromise — without needing any insider knowledge of the site.
REAL-WORLD EXAMPLE	Example: Automated bots constantly scan the internet for paths like /cpanel/. A business that left a default admin URL accessible was compromised when a bot found it, brute-forced a weak password in minutes, and installed backdoor malware — all without any human attacker being involved.
HOW TO FIX	Restrict access to /cpanel/ by IP allowlist, move it to a non-standard path, or disable it if not needed. Nginx: 'location ^~ /cpanel/ { allow YOUR_IP; deny all; }'. Also ensure strong, unique credentials are set for any admin accounts, and enable multi-factor authentication where supported.
URGENCY	**Fix immediately**
REFERENCE	CWE-284

Missing DMARC Record — Email Impersonation Risk

Port DNS · DMARC Record

HIGH

WHAT IT IS	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impersonate your business
BUSINESS RISK	This makes it significantly easier for scammers to send convincing fake emails 'from' your business — a common tactic in invoice fraud and phishing — which can directly cost your customers money and damage trust in your brand.
REAL-WORLD EXAMPLE	Example: A scammer sends an invoice-fraud email that appears to come straight from the business's own domain; with no DMARC record in place, nothing tells the recipient's mail provider the message is forged, so it lands in the inbox looking completely legitimate.
HOW TO FIX	Add a DMARC TXT record to your DNS. Go to your domain registrar's DNS settings, add a TXT record for '_dmarc' (not '@') with value: 'v=DMARC1; p=none; rua=mailto:youremail@yourdomain.com' Start at p=none — this only turns on reporting, nothing is blocked yet. Review the aggregate reports for a few weeks to confirm every legitimate mail source for this domain (email provider, helpdesk, marketing tools, etc.) is passing DMARC alignment, then move to p=quarantine, and finally p=reject once you're confident nothing legitimate will be caught. Verify at https://mxtoolbox.com/dmarc.aspx
URGENCY	**Fix immediately**
REFERENCE	CWE-290 — Authentication Bypass by Spoofing The login or identity check can be tricked by faking trusted information, letting an attacker in without real credentials.

HTTP Not Redirecting to HTTPS

Port HTTP · HTTPS Redirect

MEDIUM

WHAT IT IS	Visiting http:// doesn't redirect to https:// — some visitors may use an unencrypted connection without knowing
BUSINESS RISK	Anyone who types or clicks an http:// link is sending their activity on your site — potentially including form data or passwords — unencrypted, where it can be read by anyone on the same public wifi or compromised network.
REAL-WORLD EXAMPLE	Example: A customer types the domain into their browser without 'https://', lands on the unencrypted version of the site, and submits a form before ever reaching the secure page — sending that data in plain text the whole time.
HOW TO FIX	Add a permanent redirect from HTTP to HTTPS. Nginx: add 'return 301 https://$host$request_uri;' in your port 80 server block. Apache: add 'RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]' in your .htaccess. Cloudflare users: go to SSL/TLS > Edge Certificates > enable 'Always Use HTTPS'.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-319 — Cleartext Transmission of Sensitive Information Sensitive data is sent over the network unencrypted, so anyone monitoring the connection can read it.

Missing HSTS Header

Port HTTPS · HSTS Header

MEDIUM

WHAT IT IS	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visitors open to downgrade attacks
BUSINESS RISK	An attacker on the same network as a visitor (public wifi, a compromised router, etc.) can trick their browser into using the insecure version of your site and intercept what they type — raising the odds of stolen logins or payment details.
REAL-WORLD EXAMPLE	Example: An attacker on a shared network intercepts a visitor's first request (which defaults to HTTP) before the redirect happens, and silently serves them a fake version of the page instead of the real site.
HOW TO FIX	Add the HSTS header to your web server. Nginx: add 'add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;' in your server block. Apache: add 'Header always set Strict-Transport-Security "max-age=31536000"' in your config. Cloudflare: SSL/TLS > Edge Certificates > enable HTTP Strict Transport Security.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-319 — Cleartext Transmission of Sensitive Information Sensitive data is sent over the network unencrypted, so anyone monitoring the connection can read it.

Missing Clickjacking Protection (X-Frame-Options)

Port HTTPS · Clickjacking Protection

MEDIUM

WHAT IT IS	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick users into unwanted actions
BUSINESS RISK	An attacker could trick your customers into clicking hidden buttons — like 'change password' or 'confirm purchase' — without realizing it, potentially leading to account takeovers or unauthorized actions carried out under your brand's name.
REAL-WORLD EXAMPLE	Example: An attacker embeds the site's 'delete account' or 'confirm payment' button inside an invisible iframe on their own page, disguised under something like a fake 'play video' button — a visitor's real click triggers the hidden action on your site.
HOW TO FIX	Add the X-Frame-Options header. Nginx: 'add_header X-Frame-Options "SAMEORIGIN" always;' Apache: 'Header always set X-Frame-Options SAMEORIGIN' This tells browsers to only allow your site to be framed by pages on the same domain.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-1021 — Improper Restriction of Rendered UI Layers (Clickjacking) The site doesn't prevent itself from being embedded inside another page, which attackers can exploit to trick users into clicking something they didn't intend to.

Missing Content-Security-Policy (CSP)

Port HTTPS · Content Security Policy

MEDIUM

WHAT IT IS	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross-site scripting weakness exists elsewhere it's easier to exploit; this finding on its own doesn't mean an XSS vulnerability exists on this site
BUSINESS RISK	CSP is a defense-in-depth browser control, not evidence of an active vulnerability by itself — but if an attacker ever manages to slip malicious script onto your site through some other weakness (e.g. a vulnerable plugin or a comment field), a good CSP is often what stops that script from running and stealing customer data such as login sessions or payment details. Without it, that second layer of protection isn't there.
REAL-WORLD EXAMPLE	Example: A vulnerable comment form or compromised ad widget lets an attacker inject a script tag; with a properly scoped CSP in place, the browser would refuse to run it — without CSP, that same injected script runs freely and can forward a visitor's session cookie to the attacker.
HOW TO FIX	Add a Content-Security-Policy header, but roll it out carefully — a misconfigured CSP can break legitimate scripts/styles on the site. Start by deploying it in Report-Only mode first, which reports violations without blocking anything: 'add_header Content-Security-Policy-Report-Only "default-src \'self\'; script-src \'self\'; object-src \'none\'; report-uri /csp-report";' Review the reports for a while to catch anything the policy would break, adjust the policy, then switch the header name to 'Content-Security-Policy' (without '-Report-Only') to start enforcing it. For WordPress or complex sites, use https://csp-evaluator.withgoogle.com to help build the policy.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Apache Server Status Exposed (Unconfirmed)

Port HTTPS · Apache Server Status Exposed

MEDIUM

WHAT IT IS	The path /server-status returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms *something* is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes internal server diagnostic information, not a login panel
BUSINESS RISK	This page reveals internal details about the server's configuration, active connections, or recent errors — not something the general public should be able to see, and useful reconnaissance an attacker can use to plan a more targeted attack elsewhere on the site.
REAL-WORLD EXAMPLE	Example: An attacker reviews this page to learn internal server details, request patterns, or recent error messages, then uses that information to plan a more targeted attack elsewhere on the site instead of guessing blind.
HOW TO FIX	Restrict access to /server-status by IP allowlist, or disable it entirely if not needed. Nginx: 'location ^~ /server-status { allow YOUR_IP; deny all; }'. Apache ('server-status'/'server-info'): add 'Require ip YOUR_IP' inside the relevant <Location> block, or remove the module if unused.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-200 — Exposure of Sensitive Information The system reveals information to someone who shouldn't have access to it.

Missing MIME Sniffing Protection

Port HTTPS · MIME Sniffing

LOW

WHAT IT IS	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content injection
BUSINESS RISK	This is a minor gap on its own, but it slightly raises the odds that a malicious file could be misread as something else by a visitor's browser, helping a separate attack succeed.
REAL-WORLD EXAMPLE	Example: A user-uploaded file intended to be harmless (like an image) is reinterpreted by the browser as executable script because the server never told it what the file actually was, letting an unrelated vulnerability turn into a working attack.
HOW TO FIX	Add: 'add_header X-Content-Type-Options "nosniff" always;' (Nginx) or 'Header always set X-Content-Type-Options nosniff' (Apache). This is a one-line fix that takes 2 minutes.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Missing Referrer-Policy Header

Port HTTPS · Referrer Policy — LOW

WHAT IT IS	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party sites your pages link to
BUSINESS RISK	If any of your page addresses contain sensitive details (like a password-reset token or account ID), that information could leak to outside sites your pages link to — a small but easily avoidable privacy gap.
REAL-WORLD EXAMPLE	Example: A customer clicks an outbound link from a page whose URL happens to include an account ID or a password-reset token, and that full address — token included — is handed to the destination site in the Referer header.
HOW TO FIX	Add: 'add_header Referrer-Policy "strict-origin-when-cross-origin" always;' (Nginx) or 'Header always set Referrer-Policy strict-origin-when-cross-origin' (Apache).
URGENCY	**Fix within 1 month**
REFERENCE	CWE-16 — Configuration The weakness comes from how the software was configured, not from a flaw in its code.

Missing Permissions-Policy Header

Port HTTPS · Permissions Policy — LOW

WHAT IT IS	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricted for embedded third-party scripts
BUSINESS RISK	If you ever embed third-party ads, widgets, or analytics scripts, they could request a visitor's camera, microphone, or location without you intending to allow it — an avoidable privacy risk for your customers.
REAL-WORLD EXAMPLE	Example: An embedded ad network's script requests the visitor's location or microphone access through a permission prompt the site owner never intended to allow, simply because nothing in the page's headers restricted it.
HOW TO FIX	Add: 'add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;' Adjust based on what your site actually uses. This limits what ad/analytics scripts can access.
URGENCY	**Monitor**
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Exposed .DS_Store File

Port FILE · Information Disclosure — LOW

WHAT IT IS	a macOS .DS_Store file is publicly accessible, which can reveal the names of other files in the same folder
BUSINESS RISK	This file can list the names of other files on the server in the same folder, sometimes giving an attacker hints about other things to probe for.
REAL-WORLD EXAMPLE	Example: An attacker parses this file to see the names of other files in the same folder — sometimes turning up a backup file or admin script that was never meant to be discoverable.
HOW TO FIX	Delete the file and add a server rule to block it. Nginx: 'location ~ /\.DS_Store$ { deny all; }'.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-552 — Files or Directories Accessible to External Parties Files that should be private can be reached by people who shouldn't have access to them.

Protected Path — /.htpasswd

Port PATH · Content Discovery — LOW

WHAT IT IS	/.htpasswd returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.htpasswd returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
HOW TO FIX	No action needed if this is intentionally restricted. Confirm the credentials protecting it are strong and not left at a default.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-284

Protected Path — /server-status

Port PATH · Content Discovery

LOW

WHAT IT IS	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
HOW TO FIX	No action needed if this is intentionally restricted. Confirm the credentials protecting it are strong and not left at a default.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-284

Protected Path — /error_log

Port PATH · Content Discovery

LOW

WHAT IT IS	/error_log returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/error_log returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
HOW TO FIX	No action needed if this is intentionally restricted. Confirm the credentials protecting it are strong and not left at a default.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-284

No Abuse Reports Found for Public IP

Port HTTPS · IP Reputation

INFO

WHAT IT IS	Public IP 108.179.252.18 (hosted by Oracle Corporation) has no abuse reports on AbuseIPDB in the last 90 days.
BUSINESS RISK	A clean IP reputation is a good sign — no other indication needed here.
HOW TO FIX	No action required.
URGENCY	**Informational**

Hosting Network Identified

Port HTTPS · IP WHOIS / Network Ownership

INFO

WHAT IT IS	Public IP 108.179.252.18 is registered to HostGator.com LLC — network: HGBLOCK-5 — block: 108.179.192.0 – 108.179.255.255.
BUSINESS RISK	This is informational — it tells you (and anyone else who looks it up) which hosting provider or network actually operates this IP. Useful for confirming you're hosted where you expect, or for context if the IP reputation check above flags anything.
HOW TO FIX	No action required — this is identifying information, not a vulnerability.
URGENCY	Informational

Path Discovered — /.DS_Store

Port PATH · Content Discovery

INFO

WHAT IT IS	/.DS_Store returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/.DS_Store returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
HTTPS	cPanel Exposed	HIGH	The path /cpanel/ is accessible without authentication — this exposes administration functionality t
DNS	DMARC Record	HIGH	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impers
HTTP	HTTPS Redirect	MEDIUM	Visiting http:// doesn't redirect to https:// — some visitors may use an unencrypted connection with
HTTPS	HSTS Header	MEDIUM	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visit

HTTPS	Clickjacking Protection	**MEDIUM**	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick us
HTTPS	Content Security Policy	**MEDIUM**	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross
HTTPS	Apache Server Status Exposed	**MEDIUM**	The path /server-status returns a restricted-access response (401/403) that is genuinely distinct fr
HTTPS	MIME Sniffing	**LOW**	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content
HTTPS	Referrer Policy	**LOW**	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party s
HTTPS	Permissions Policy	**LOW**	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
FILE	Information Disclosure	**LOW**	a macOS .DS_Store file is publicly accessible, which can reveal the names of other files in the same
PATH	Content Discovery	**LOW**	/.htpasswd returned HTTP 403. This confirms the path exists, but access control prevented access — i
PATH	Content Discovery	**LOW**	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access
PATH	Content Discovery	**LOW**	/error_log returned HTTP 403. This confirms the path exists, but access control prevented access — i
HTTPS	IP Reputation	**INFO**	Public IP 108.179.252.18 (hosted by Oracle Corporation) has no abuse reports on AbuseIPDB in the las
HTTPS	IP WHOIS / Network Ownership	**INFO**	Public IP 108.179.252.18 is registered to HostGator.com LLC — network: HGBLOCK-5 — block: 108.179.19
PATH	Content Discovery	**INFO**	/.DS_Store returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa

NEXT STEPS

→ Start with the 2 HIGH risk finding(s) today — these are your most urgent risks. First, address 'cPanel Exposed': Restrict access to /cpanel/ by IP allowlist, move it to a non-standard path, or disable it if not needed. Then work through the remaining findings in order of severity.