connvertex

SAMPLE REPORT
Fictional client, illustration only

OFFENSIVE SECURITY · ENGAGEMENT REPORT · v1.0

Penetration Test Report

External network + web application assessment

PREPARED FOR

Federal Program Services Bureau
U.S. federal civilian agency (fictional — for illustration only)

ENGAGEMENT
External Network + Web Application Penetration Test

WINDOW
2026-02-02 to 2026-02-20 (3 weeks)

REPORT ISSUED
2026-03-04

VERSION
1.0 · FINAL

CLASSIFICATION — **CONFIDENTIAL — FPSB & Connvertex only**

Prepared by Connvertex · Practitioner-led cybersecurity consulting for government. connvertex.com · hello@connvertex.com

SECTION 01

Document control

Classification, revision history, approvals, and the disclaimer that scopes how this report can be used.

Revision history

Version	Date	Author	Summary of change
0.1 DRAFT	2026-02-24	Connvertex Offensive Security	Initial findings walk-through with FPSB CISO office.
0.5 DRAFT	2026-02-27	Connvertex Offensive Security	Incorporated FPSB feedback on CVX-2026-001 and CVX-2026-004 impact framing.
0.9 DRAFT	2026-03-02	Connvertex Principal (independent QA)	QA pass; added Privacy Act framing to Exec Summary; adjusted CVSS on CVX-2026-005.
1.0 FINAL	2026-03-04	Connvertex Offensive Security	Final issuance to FPSB; retest window opens per SLA.

Distribution & approvals

Role	Name	Organization
Engagement lead (deliverable owner)	[Lead Practitioner on file]	Connvertex
Independent QA reviewer	[Principal on file]	Connvertex
Client executive sponsor	[FPSB CISO on file]	Federal Program Services Bureau
Client technical POC	[FPSB Security Architect on file]	Federal Program Services Bureau
Authorized recipients	FPSB CISO office; FPSB Application Engineering leads; Connvertex engagement team.	—

Disclaimer and handling

This report documents a specific engagement at a specific point in time. Controls, configurations, and attack surfaces change; the absence of a finding here does not imply the absence of risk in the same area at a later date. The report is issued to the authorized recipients listed above and to personnel with a need-to-know inside those organizations. External distribution — including to auditors, insurers, or agency partners — requires written approval from the FPSB CISO office.

Sample notice. This document is a **sample** produced by Connvertex to demonstrate deliverable quality. The client, dataset, hosts, IP ranges, CVEs, and evidence snippets are fictional or have been replaced with RFC 5737 / RFC 3849 / example.com equivalents. The format, depth, and process described are representative of a real Connvertex engagement.

SECTION 02

Contents

This report is designed to be read end-to-end by technical leadership and excerpted by section for operational teams. Each detailed finding is self-contained: an executive-grade summary, reproduction evidence, business impact, and a remediation sequence with owners.

SECTION 03

Executive summary

A two-page read-out for leadership, a severity distribution dashboard, and the recommended next steps.

Posture statement

FPSB's external attack surface is well-segmented but contains two critical exposures that materially change the risk posture: an unauthenticated SQL injection on a citizen-facing case-lookup endpoint, and an administrative interface reachable from the public internet with credentials that were never rotated from the vendor default. Either finding, exploited in isolation, would support exfiltration of Personally Identifiable Information (PII) covered by the Privacy Act of 1974 and produce a reportable incident under OMB M-17-12. Chained, the two provide a reliable path from the public internet to agency records inside of one business day. The balance of the findings describe preventable hygiene gaps — unpatched perimeter software, insecure direct object references, weak TLS configuration, and an authenticated-spoofing path against the fpsb.gov sender domain — that are individually manageable but collectively indicate a program operating without continuous attack-surface review.

Findings at a glance

Distribution by severity

Top risks to act on this week

#	Finding	Severity	CVSS	Why now
1	Unauthenticated SQL injection on cases.fpsb.gov	Critical	9.8	Directly exfiltrates Privacy-Act-protected records with no credentials.
2	Default creds on admin-legacy.fpsb.gov	Critical	9.6	One-click path to the same dataset; no injection required.

3	Unpatched VPN appliance (KEV-listed)	High	7.5	In-the-wild exploitation; patches available; trivial to confirm externally.

Recommended sequence

Within 24 hours. Confirm the WAF rule deployed for CVX-2026-001 is on and monitored; apply an IP allowlist on admin-legacy.fpsb.gov; open the change record to deploy the VPN firmware.

Within 14 days. Replace the vulnerable case-lookup handler with parameterized queries; rotate and federate all admin credentials; deploy the VPN patch; remediate the partner API authorization check.

Within 60 days. Close the remaining hygiene findings (TLS, HSTS, DMARC, security headers); add continuous external attack-surface monitoring; schedule a full retest.

SECTION 04

Engagement overview

Client, objectives, in-scope assets, out-of-scope boundaries, engagement team, and operating assumptions.

CLIENT	**Federal Program Services Bureau** (FPSB) U.S. federal civilian agency (fictional — for illustration only)
ENGAGEMENT	External Network + Web Application Penetration Test
WINDOW	2026-02-02 to 2026-02-20 (3 weeks)
PRIMARY DOMAIN	`fpsb.gov (sample)`
LEAD TESTER	Senior Offensive Security Consultant, Connvertex
SUPPORT TESTER	Web Application Security Specialist, Connvertex
QA REVIEWER	Principal Security Consultant, Connvertex (independent QA)
CLIENT POC	FPSB CISO Office (name on file)

Objectives

FPSB engaged Connvertex to (1) measure the exploitability of its public-facing attack surface from the perspective of an unauthenticated external attacker, (2) exercise the partner portal with authenticated low-privilege and read-only test accounts to surface authorization-class findings, and (3) produce a written deliverable suitable for direct inclusion in FPSB's POA&M and for sharing with auditors with a need-to-know.

IN SCOPE	OUT OF SCOPE

- fpsb.gov and all first-level subdomains discoverable via passive reconnaissance
- 203.0.113.0/24 — FPSB external allocation (RFC 5737 documentation range, substituted)
- Public citizen-facing web applications at cases.fpsb.gov and forms.fpsb.gov
- Authenticated testing of the FPSB partner portal at partners.fpsb.gov using two test accounts issued by FPSB
- Email authentication posture (SPF, DKIM, DMARC) for fpsb.gov and fpsb-mail.gov
- External DNS and TLS configuration for all in-scope hosts

- Denial-of-service testing of any form (agreed in the Rules of Engagement)
- Social engineering of FPSB personnel; no phishing or pretexting was attempted
- Physical facility intrusion; all testing was conducted remotely from Connvertex-controlled egress
- Any system inside the FPSB .gov internal allocation not explicitly listed above
- Third-party SaaS (Salesforce Government Cloud, ServiceNow) — covered by separate third-party attestations
- Source-code review; black-box / grey-box perspective only

Operating assumptions

- Testing windows were 08:00–20:00 ET weekdays and 10:00–16:00 ET Saturdays. All testing outside those windows required written approval from the FPSB CISO.
- Connvertex egress IP addresses 198.51.100.14 and 198.51.100.15 were allowlisted through FPSB WAF and mail gateway for the duration of the engagement.
- Any exploit confirmed was halted immediately after sufficient proof-of-concept was captured; no data was exfiltrated beyond what is reproduced in the evidence blocks in this report.
- Two FPSB staff accounts (one Contributor, one Read-Only) were issued for authenticated testing and are to be disabled at report acceptance.

SECTION 05

Methodology

The phased workflow, standards-alignment, and tooling used across the engagement.

Phase	What we did	Primary tools
Reconnaissance	Passive collection of external metadata: DNS records, certificate transparency logs, ASN/CIDR attribution, public sharing platforms (GitHub, Pastebin, Slideshare), WHOIS history, and employee attribution from public sources. No traffic was sent to FPSB-operated systems during this phase.	`OSINT Framework · Amass · crt.sh · Shodan · theHarvester`
Enumeration & Mapping	Active but non-invasive probing of the in-scope CIDR ranges and discovered hostnames. Service fingerprinting, virtual-host discovery, subdomain brute-forcing against observed naming patterns, TLS inspection, and HTTP method enumeration.	`Nmap 7.95 · Masscan · Aquatone · Nuclei · feroxbuster`
Vulnerability Identification	Authenticated and unauthenticated identification of known CVE exposures, configuration weaknesses, and application-layer logic flaws. Web applications were exercised manually against the OWASP Web Security Testing Guide (v4.2) and the OWASP API Security Top 10 (2023).	`Burp Suite Professional · sqlmap · Nuclei · ZAP · Nessus Professional`
Exploitation	Validated exploit chains to confirm real-world impact, with each chain halted at the earliest evidence that established exploitability. Every exploited path was logged, timestamped, and paired with a recoverable-state confirmation ticket to FPSB operations.	`Burp Suite · sqlmap · custom Python PoCs · Metasploit (selective)`
Post-Exploitation (bounded)	For confirmed exploits, a minimum-privilege pivot was demonstrated to establish blast radius — e.g., enumerating accessible tables, listing readable filesystem paths, or demonstrating lateral reachability — without altering data or persisting access.	`Bash · PowerShell · Responder (listen-only) · impacket (selective)`
Reporting & Evidence Collation	Findings were normalized to CVSS v3.1 scoring, mapped to NIST SP 800-53 Rev 5 controls, MITRE ATT&CK; techniques, and the Privacy Act / OMB M-17-12 obligations relevant to the affected data classes. Evidence was captured in a dedicated engagement repository with hash-verified artifacts.	`Markdown · Obsidian · custom Python ETL to CVSS calculator`

Standards and frameworks referenced

PTES — Penetration Testing Execution Standard	**OWASP Web Security Testing Guide v4.2 (WSTG)**	**OWASP Application Security Verification Standard (ASVS 4.0.3)**	**OWASP API Security Top 10 (2023)**
NIST SP 800-115 — Technical Guide to Information Security Testing	**NIST SP 800-53 Rev 5 — Security and Privacy Controls**	**MITRE ATT&CK; Enterprise Matrix v15**	**CVSS v3.1 for severity scoring**

SECTION 06

Risk rating framework

How every finding in this report was scored, and the remediation SLA that applies at each severity.

Severity	CVSS	Definition	Response SLA
CRITICAL	9.0 – 10.0	Directly exploitable with low attacker skill, affecting confidentiality, integrity, or availability of regulated data or agency operations. Exploit either observed during testing or trivial to weaponize.	Begin remediation within 24 hours; mitigating control applied within 72 hours; permanent fix within 14 days.
HIGH	7.0 – 8.9	Exploitable with moderate attacker skill or under common conditions; material impact on regulated data or operational continuity. Typically requires chaining with a second finding to reach full impact.	Begin remediation within 3 business days; permanent fix within 30 days.
MEDIUM	4.0 – 6.9	Exploitation requires specific conditions or meaningful skill; limited or indirect impact on regulated data, or direct impact on less-sensitive systems. Hygiene-class findings live here.	Begin remediation within 10 business days; permanent fix within 60 days.
LOW	0.1 – 3.9	Low likelihood or low impact in isolation; typically best-practice or defense-in-depth gaps.	Address in the next routine release cycle; document acceptance if not remediated within 90 days.
INFO	0.0	No exploitability under current conditions; captured to inform future hardening or monitoring.	No remediation SLA; track for trend analysis.

All CVSS scores in this report are calculated against CVSS v3.1 base metrics. Temporal and environmental adjustments are noted inline where they alter the base score materially. Where an FPSB-specific environmental factor changes priority despite a lower base score (e.g., a low-CVSS finding that touches Privacy-Act data), that context is called out in the finding's Business impact section.

SECTION 07

Findings summary

Ten findings identified during the engagement, ordered by severity. Six are documented in detail; four are hygiene-class issues summarized in the table.

ID	Severity	CVSS	Finding	Affected
CVX-2026-001	CRITICAL	9.8	**Unauthenticated SQL injection on citizen case-lookup endpoint**	https://cases.fpsb.gov/api/v1/lookup
CVX-2026-002	CRITICAL	9.6	**Administrative interface reachable from public internet with vendor default credentials**	https://admin-legacy.fpsb.gov:8443/
CVX-2026-003	HIGH	8.1	**Insecure direct object reference in partner records API**	https://partners.fpsb.gov/api/v2/records/{record_id}
CVX-2026-004	HIGH	7.5	**Unpatched perimeter service — known-exploitable CVE in public VPN appliance**	vpn.fpsb.gov (203.0.113.42)
CVX-2026-005	MEDIUM	5.3	**Weak TLS configuration and missing HSTS on citizen-facing hosts**	cases.fpsb.gov forms.fpsb.gov partners.fpsb.gov
CVX-2026-006	MEDIUM	5.0	**Email spoofing possible — DMARC policy set to p=none on the primary sender domain**	fpsb.gov fpsb-mail.gov
CVX-2026-007	LOW	3.7	**Security headers partially deployed** Remediation: Set Content-Security-Policy, X-Frame-Options, Referrer-Policy, and Permissions-Policy on all citizen-facing hosts.	cases.fpsb.gov · forms.fpsb.gov
CVX-2026-008	LOW	3.1	**Verbose error messages leak stack traces** Remediation: Suppress stack traces from HTTP responses; log to the SIEM instead.	cases.fpsb.gov
CVX-2026-009	INFO	0.0	**Legacy certificate authority still trusted by internal CA chain** Remediation: Track for removal at the next PKI refresh; no exploitable path today.	Agency-internal CA

CVX-2026-010	INFO	0.0	**Sensitive information in HTML comments on legacy marketing microsite** Remediation: Strip legacy HTML comments at next CMS release.	about.fpsb.gov

SECTION 08

Detailed findings

Six findings documented in full. Each is self-contained so sections can be excerpted and routed to the responsible owner.

FINDING 01 · CVX-2026-001	CRITICAL · CVSS 9.8

Unauthenticated SQL injection on citizen case-lookup endpoint

CVSS VECTOR	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
OWASP	A03:2021 Injection
NIST SP 800-53	SI-10 · SC-7 · AC-3 · SI-3
MITRE ATT&CK	T1190 Exploit Public-Facing Application · T1565 Data Manipulation
STATUS	OPEN — patched during engagement (interim WAF rule); permanent fix pending
AFFECTED	`https://cases.fpsb.gov/api/v1/lookup`

Summary

The public case-lookup endpoint accepts a `case_id` query parameter that is concatenated directly into the SQL WHERE clause executed against the Cases database. A time-based blind SQL injection was confirmed; a boolean-based proof-of-concept returned the currently authenticated database user, version, and schema enumeration within 40 minutes of first probe. The endpoint is reachable without authentication.

Business impact

An attacker with no credentials can enumerate and exfiltrate the Cases table, which we confirmed contains name, address, date-of-birth, partial SSN, and benefits case status for FPSB beneficiaries. The dataset falls within the Privacy Act's 'system of records' definition; a successful exfiltration would constitute a reportable major incident under OMB M-17-12 (one-hour CISA notification) and likely trigger Congressional reporting.

Privacy hook. Privacy Act of 1974 (5 U.S.C. § 552a); reporting obligation under OMB M-17-12.

Evidence (sanitized)

```
# Request (sanitized; parameters altered)
GET /api/v1/lookup?case_id=24%20AND%20SLEEP(5)-- HTTP/1.1
Host: cases.fpsb.gov
User-Agent: cvx-offsec/1.0

# Response (excerpt)
HTTP/1.1 200 OK
Content-Type: application/json
X-Response-Time: 5012ms ← note the 5 second delay

# sqlmap confirmation (bounded; --level=3, --risk=2, no DB drop)
[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[INFO] GET parameter 'case_id' is 'MySQL >= 5.0.12 time-based blind' injectable
back-end DBMS: MySQL >= 5.0.12
current user: 'fpsb_cases_rw'@'10.42.7.%'
available databases (7): [information_schema, cases, crm, dim_lookup, mysql, perf, sys]

# Row counts (enumeration halted here by RoE)
cases.case_header → 2,482,106 rows
cases.claimant_pii → 2,201,874 rows
```

Remediation

- Short-term (within 24 hours, deployed during engagement): WAF rule blocking OR/AND/UNION/SLEEP tokens in the `case_id` parameter at the perimeter. Validated to block every PoC payload in our library.
- Medium-term (within 14 days): Re-implement the handler using parameterized queries via the agency's standard ORM layer. Remove the current string-concatenation path.
- Long-term (within 60 days): Enable RASP-class monitoring on the Cases API and add a canary query detection rule in the SIEM for unusual WHERE-clause patterns. Schedule retest.

References

- OWASP Cheat Sheet: SQL Injection Prevention
- CWE-89: SQL Injection
- NIST SP 800-53 Rev 5: SI-10 Information Input Validation

FINDING 02 · CVX-2026-002 | CRITICAL · CVSS 9.6

Administrative interface reachable from public internet with vendor default credentials

CVSS VECTOR	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L`
OWASP	A07:2021 Identification and Authentication Failures
NIST SP 800-53	IA-5 · AC-7 · SC-7 · CM-6
MITRE ATT&CK	T1078.001 Valid Accounts: Default Accounts · T1133 External Remote Services
STATUS	OPEN — access restricted by IP allowlist during engagement; permanent auth redesign pending
AFFECTED	`https://admin-legacy.fpsb.gov:8443/`

Summary

A second-generation administrative console (`admin-legacy.fpsb.gov`) is reachable on the public internet and accepted the vendor default credentials documented in the product's installation guide. The console is paired with the same Cases database affected by Finding CVX-2026-001 and provides direct record export.

Business impact

The default credentials grant Application Administrator rights. From the admin console an attacker can (a) export the full Cases table, (b) create additional administrative users and (c) pivot to the Cases API management plane. The same scope of data as CVX-2026-001 is reachable with no injection required.

Privacy hook. Access to admin-legacy indirectly grants read access to the Cases dataset.

Evidence (sanitized)

```
# HTTPS banner
curl -skI https://admin-legacy.fpsb.gov:8443/
HTTP/1.1 200 OK
Server: CaseConsole/2018.3
X-Powered-By: Vendor-Admin-Kit 4.8

# Login (exact screen text redacted; credentials from public install guide)
POST /auth/login HTTP/1.1
Host: admin-legacy.fpsb.gov:8443
Content-Type: application/x-www-form-urlencoded
username=admin&password=<vendor default>

HTTP/1.1 302 Found
Location: /console/home
Set-Cookie: CCSESSION=<redacted>; HttpOnly; Secure

# Role after successful login (JSON trimmed)
{ "user": "admin", "roles": ["ApplicationAdministrator"],
"allowedActions": ["EXPORT_RECORDS", "MANAGE_USERS", "MANAGE_API_KEYS"] }
```

Remediation

- Immediate: enforce Connvertex-supplied IP allowlist at the F5 VIP; this was applied within four hours of reporting and validated at retest.
- Short-term (7 days): rotate all administrative passwords and remove every vendor-default account. Enforce SSO via the agency's PIV/CAC-integrated identity provider.
- Medium-term (30 days): move admin-legacy behind the agency's standard Zero Trust proxy; disable direct internet exposure. Add a CM-6 baseline entry banning public exposure of any `admin*.fpsb.gov` host.
- Long-term: decommission the 2018 admin stack in favor of the agency's standard admin control plane per the modernization roadmap; target 2026 Q3.

References

- CIS Control 5.2 — No use of default credentials
- NIST SP 800-63B — Authenticator Assurance Level guidance

FINDING 03 · CVX-2026-003 | HIGH · CVSS 8.1

Insecure direct object reference in partner records API

CVSS VECTOR	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
OWASP	A01:2021 Broken Access Control
NIST SP 800-53	AC-3 · AC-6 · AU-2
MITRE ATT&CK	T1190 · T1212 Exploitation for Credential Access (authorization-scope variant)
STATUS	OPEN — triaged
AFFECTED	https://partners.fpsb.gov/api/v2/records/{record_id}

Summary

The partner records API enforces authentication but not authorization on the `/records/{record_id}` path. A Contributor-role test account was able to fetch records belonging to three other partner organizations by incrementing the integer record_id parameter. No tenant isolation check is performed server-side.

Business impact

A compromised or malicious partner account can enumerate and read records across all FPSB partner organizations. The endpoint returns case-referral metadata including beneficiary identifiers, partner names, and service notes. Cross-partner exposure breaches FPSB's minimum-necessary policy and creates partner-confidentiality exposure.

Privacy hook. Cross-partner disclosure violates the minimum-necessary rule.

Evidence (sanitized)

```
# Authenticated fetch with low-privilege test account (partner A)
GET /api/v2/records/10482 HTTP/1.1
Host: partners.fpsb.gov
Authorization: Bearer <token for partner A, Contributor role>

HTTP/1.1 200 OK
Content-Type: application/json
{"record_id":10482,"owning_partner":"PARTNER_D","subject_initials":"J.R.",
"service_notes":"[REDACTED — 214 bytes]","case_ref":"FPSB-2025-884219"}

# Decrement & increment confirmed the same behavior across record_id 10450..10500
# 38 of 51 records belonged to partners other than PARTNER_A.
```

Remediation

- Enforce partner-ownership check on every `/records/*` call — reject with 403 when `owning_partner` does not match the JWT's partner claim.

- Replace predictable integer record_id with UUIDv7 or ULID in a backwards-compatible window, and publish a deprecation notice on the public API changelog.
- Add an AU-2 audit event for every cross-partner read attempt, with a SIEM rule that alerts on >5 cross-partner denials from a single token in 60 seconds.

References

- OWASP API Security Top 10 2023: API1 Broken Object Level Authorization
- NIST SP 800-53 Rev 5: AC-3(7) Role-Based Access Control

FINDING 04 · CVX-2026-004 | HIGH · CVSS 7.5

Unpatched perimeter service — known-exploitable CVE in public VPN appliance

CVSS VECTOR	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
OWASP	n/a (infrastructure)
NIST SP 800-53	SI-2 · CM-8 · RA-5
MITRE ATT&CK	T1190 Exploit Public-Facing Application
STATUS	OPEN — vendor patch available; deployment scheduled
AFFECTED	vpn.fpsb.gov (203.0.113.42)

Summary

The FPSB remote-access VPN endpoint is running a firmware release that predates the vendor's advisory for a disclosed, actively-exploited information-disclosure vulnerability. A safe version banner was captured; exploitation was not attempted under the Rules of Engagement, but the vulnerable version is trivial to confirm.

Business impact

Public advisories and commercially tracked threat-intelligence report active in-the-wild exploitation of this CVE against government and critical-infrastructure targets. The FPSB VPN appliance is in the path to the internal .gov allocation and is the most attractive initial-access target on the perimeter.

Privacy hook. A successful VPN exploit would grant unauthorized access to the internal allocation not in scope for this engagement.

Evidence (sanitized)

```
$ nmap -sV -p 443 --script http-headers vpn.fpsb.gov
443/tcp open ssl/https
| http-server-header: [Vendor VPN Appliance] 9.1R8.2
| Subject: CN=vpn.fpsb.gov
| Issuer: CN=DigiCert TLS RSA SHA256 2020 CA1

Advisory cross-ref:
- Vendor bulletin published 2025-11-14 (patched in 9.1R11 and 22.4R3)
- CISA KEV catalog entry 2025-11-20 (exploited in the wild)
- EPSS score 0.93 (high exploit probability) at time of report
```

Remediation

- Deploy vendor firmware 22.4R3 or 9.1R11.3 during the next maintenance window. The vendor has published a non-disruptive upgrade procedure for in-place upgrades.

- Confirm against the CISA KEV catalog weekly; route catalog deltas into the vulnerability management ticket queue (RA-5 / SI-2 linked).
- Enable the appliance's built-in syslog feed into the agency SIEM and add a detection rule for the IOCs published in the vendor bulletin.

References

- CISA Known Exploited Vulnerabilities Catalog
- NIST SP 800-53 Rev 5: SI-2 Flaw Remediation
- Vendor security advisory (bulletin ID on file)

FINDING 05 · CVX-2026-005 | MEDIUM · CVSS 5.3

Weak TLS configuration and missing HSTS on citizen-facing hosts

CVSS VECTOR	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
OWASP	A02:2021 Cryptographic Failures
NIST SP 800-53	SC-8 · SC-13 · SC-23
MITRE ATT&CK	T1557 Adversary-in-the-Middle (downgrade variant)
STATUS	OPEN
AFFECTED	cases.fpsb.gov forms.fpsb.gov partners.fpsb.gov

Summary

Three citizen-facing hostnames still accept TLS 1.0 and TLS 1.1 and present CBC cipher suites first. None of the three return a `Strict-Transport-Security` response header, so downgrade to HTTP is possible on first-visit. The FedRAMP Moderate baseline requires TLS 1.2 or higher using FIPS-validated modules; TLS 1.0/1.1 deprecation was mandated across federal civilian agencies by BOD 20-01.

Business impact

Citizens on adversary-controlled networks — hotel Wi-Fi, conference venues, mobile-data MITM — can have form submissions intercepted or modified before TLS is locked in. The risk is low in absolute terms but disproportionately visible if exploited given the public-facing surface.

Privacy hook. A successful downgrade on a citizen-facing form permits PII interception on hostile networks.

Evidence (sanitized)

```
$ testssl.sh --warnings off cases.fpsb.gov
Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (NOT ok)
TLS 1.1 offered (NOT ok)
TLS 1.2 offered (OK), final
TLS 1.3 not offered

HSTS not offered
HSTS includeSubDomains not applicable

Cipher order (first 3): ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-SHA, AES256-SHA
```

Remediation

- Disable TLS 1.0 / 1.1 on all three hosts. Prefer TLS 1.3 where the load-balancer supports it; otherwise, AEAD cipher suites on TLS 1.2.
- Set `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` on all citizen-facing hosts and submit the top-level domain to the HSTS preload list.
- Retest with testssl.sh and the ssllabs API after deployment; target an overall grade A.

References

- CISA BOD 20-01 (TLS 1.0/1.1 deprecation)
- NIST SP 800-52 Rev 2 — Guidelines for TLS Implementations

FINDING 06 · CVX-2026-006 | MEDIUM · CVSS 5.0

Email spoofing possible — DMARC policy set to p=none on the primary sender domain

CVSS VECTOR	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
OWASP	n/a (mail authentication)
NIST SP 800-53	SC-8 · SC-20 · AT-2 · AT-3
MITRE ATT&CK	T1566 Phishing · T1078 Valid Accounts (social-engineered)
STATUS	OPEN
AFFECTED	fpsb.gov fpsb-mail.gov

Summary

The primary sender domain fpsb.gov publishes a DMARC record with `p=none`, and the secondary sender domain fpsb-mail.gov publishes no DMARC record at all. Under BOD 18-01 federal civilian agencies were required to reach `p=reject` with subdomain coverage. Spoofed mail from fpsb.gov is therefore deliverable to recipients whose MTAs enforce DMARC; we confirmed delivery to a Connvertex-controlled test mailbox.

Business impact

Adversaries can send mail appearing to originate from any fpsb.gov address. The highest expected-value use is spear-phishing FPSB partner contacts or beneficiaries with urgent account-update lures. DMARC enforcement is a known quick-win; it is flagged here because FPSB had committed to `p=reject` in a prior internal milestone plan.

Privacy hook. Impersonation of FPSB sender addresses would materially raise phishing success rates against partners and beneficiaries.

Evidence (sanitized)

```
$ dig +short TXT _dmarc.fpsb.gov
"v=DMARC1; p=none; rua=mailto:dmarc-agg@fpsb.gov; fo=1"

$ dig +short TXT _dmarc.fpsb-mail.gov
(no record)

$ dig +short TXT fpsb.gov | grep spf
"v=spf1 ip4:203.0.113.16/28 include:_spf.salesforce.com -all"

# Delivery test (spoof with permissive MTA, from Connvertex-controlled relay)
From: Director of Operations <director@fpsb.gov>
To: <cvx-test@inbox.connvertex.sample>
Subject: [TEST] Policy update
# Message was delivered to Inbox (not Junk) by recipient's DMARC-enforcing MTA.
```

Remediation

- Move fpsb.gov from `p=none` to `p=quarantine` for two weeks, then to `p=reject` with `sp=reject` and `adkim=s; aspf=s`. Publish an aggregate report endpoint already in use.
- Publish a DMARC record for fpsb-mail.gov with an equivalent policy; ensure DKIM signing is in place on all authorized senders before enforcement.
- Enroll the primary domain in CISA's Cyber Hygiene Email Security service for ongoing DMARC monitoring and re-publishing checks.

References

- CISA BOD 18-01 — Enhance Email and Web Security
- IETF RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance

SECTION 09

Remediation roadmap

A 90-day sequence that pairs every finding with an owner role and a deadline. Meant to drop directly into FPSB's POA&M.;

0 – 30 days · Contain

- Permanent parameterized-query fix for CVX-2026-001; remove WAF-only dependency. (Owner: App Eng)
- Rotate all administrative passwords; disable vendor-default accounts; apply SSO via PIV/CAC. (Owner: IAM)
- Move admin-legacy behind Zero Trust proxy; disable internet-facing path. (Owner: Network Eng)
- Deploy VPN firmware 22.4R3 / 9.1R11.3 during next maintenance window. (Owner: Perimeter Eng)

31 – 60 days · Harden

- Enforce partner-ownership check on `/records/*`; roll out UUID record_id migration. (Owner: API Eng)
- Disable TLS 1.0/1.1 everywhere; publish HSTS preload; retest with ssllabs API. (Owner: Platform)
- Move DMARC to p=quarantine then p=reject; publish DMARC for fpsb-mail.gov. (Owner: Messaging)
- Enable RASP-class monitoring on Cases API; add canary WHERE-clause SIEM rule. (Owner: SOC)

61 – 90 days · Operate

- Stand up continuous external attack-surface monitoring with daily delta review. (Owner: SOC Lead)
- Add quarterly authenticated retest of partner API and Cases API to the engagement calendar.
- Update the agency SSP and POA&M; with every finding and close the related items.
- Run a 60-minute tabletop on a PII exfiltration scenario and capture an AAR.

SECTION 10

Retesting plan & SLA

How and when Connvertex will verify closure and how the retest ties into the engagement billing.

- Critical findings: retest within 7 calendar days of fix notification.
- High findings: retest within 14 calendar days of fix notification.
- Medium / Low: rolled into the next scheduled quarterly retest.
- Retests are free and included in the engagement scope. A one-page retest memo will be issued for each round, appended to this report as an addendum.

SECTION A

Appendix A · Tools used

The tool stack the engagement team relied on across all six phases. Versions captured at start of engagement.

Category	Tools
Reconnaissance	Amass, theHarvester, dnsrecon, Shodan CLI, crt.sh queries, GitHub code search, Wayback Machine, Aquatone
Network / service mapping	Nmap 7.95, Masscan 1.3.2, Naabu, feroxbuster 2.10, gobuster 3.6, dirsearch
TLS & cryptography	testssl.sh, sslyze, tls-scan, openssl s_client, ssllabs API
Vulnerability identification	Nuclei (v3), Nessus Professional 10.7, Qualys VMDR (read-only), Burp Suite Professional 2024.x
Web / API exploitation	Burp Suite Professional, ZAP 2.15, sqlmap 1.8, NoSQLMap, ffuf, Arjun, Postman
Password & credential testing	Hashcat 6.2 (offline-only, per RoE), hydra (selectively), CeWL
Email authentication	dmarcian (read-only), learndmarc, custom mail-header tooling
Custom tooling	Connvertex internal PoC scripts in Python 3.12; all code and artifacts retained in the engagement repository.

SECTION B

Appendix B · Glossary & references

Short definitions for the acronyms used in this report, plus a closing reading list.

Term	Meaning
ATT&CK;	MITRE's Adversarial Tactics, Techniques & Common Knowledge framework.
CVSS	Common Vulnerability Scoring System v3.1 — severity scoring model.
CUI	Controlled Unclassified Information; U.S. federal designation for regulated non-classified data.
DMARC	Domain-based Message Authentication, Reporting, and Conformance (RFC 7489).
HSTS	HTTP Strict Transport Security — forces browsers onto HTTPS for a declared period.
IDOR	Insecure Direct Object Reference — authorization flaw exposing records via predictable identifiers.
KEV	CISA's Known Exploited Vulnerabilities catalog.
PII	Personally Identifiable Information.
PTES	Penetration Testing Execution Standard.
RoE	Rules of Engagement — the signed agreement governing scope, timing, and handling.
SSP / POA&M;	System Security Plan / Plan of Action & Milestones — the federal compliance documentation pair.
WSTG	OWASP Web Security Testing Guide.

About Connvertex

Connvertex is a practitioner-led cybersecurity and digital services firm serving U.S. federal, state, and local government. Offensive security service lines include external and internal penetration testing, web and API testing, red team and Purple Team engagements, and continuous attack-surface management. **Minority-owned · Woman-owned · NMSDC MBE certified.**