Delta Intelligent Building Technologies

Cybersecurity Bulletin 2026-09-14 — enteliWEB CVE Assessment

Summary

First published: September 14, 2026

Description	A customer-supplied vulnerability scan flagged 67 CVEs against enteliWEB and related components. Delta Controls' engineering team reviewed each finding against enteliWEB's actual code paths, architecture, and deployment configuration. No critical, remotely exploitable vulnerability was identified in a standard enteliWEB deployment: 48 findings do not apply, 18 require conditions that are absent or tightly constrained in normal operation (local database access, a deprecated interface, extreme input sizes), and 1 warrants customer verification of any custom frontend code.
Products	enteliWEB, enteliSKETCH, enteliVAULT (not affected)
Recommended Action	No emergency action is required. Four proactive hardening steps are recommended: keep enteliWEB updated, as each release refreshes the bundled PHP runtime; note that the legacy SOAP interface is being removed entirely in enteliWEB 4.34; keep the bundled PostgreSQL updated on the same release and SLA cadence; and follow the enteliWEB Hardening Guide to restrict BIRT, PgJDBC, and other internal services to localhost or trusted networks.

CVE ID	CVSS Vector	Score
67 CVEs reviewed (no single CVE)	Not applicable — findings assessed individually; see Description	No critical findings

Head Office
17850 56 Ave. Surrey
BC Canada V3S 1C7

Phone/Fax
Tel +1 604.574.9444
Fax +1 604.574.7630

Web /Email
info@deltacontrols.com
www.deltacontrols.com

Delta Intelligent Building Technologies

Description

This review covers findings relevant to enteliWEB, enteliSKETCH, and enteliVAULT, deployed on Windows Server with IIS/FastCGI, PHP and Python backends, a React frontend, PostgreSQL, and the BIRT reporting engine. Findings tied to unrelated host software (e.g., Splashtop, pgAdmin4, enteliSAVE) were excluded — those are separate products, not enteliWEB components. Of the 67 CVEs in the customer-supplied scan, 48 were assessed as not affected, 18 as limited or low exposure, and 1 as warranting customer verification.

Why enteliWEB Is Not Affected

- **Legacy SOAP interface is not exposed.**
  CVE-2026-7262, CVE-2026-7261, and CVE-2026-6722 affect the deprecated PHP SOAP interface. Systems without the APPS module never expose it, and the interface is being removed entirely in enteliWEB 4.34.
- **Database services are not network-reachable.**
  The 12 PostgreSQL CVEs against the bundled PostgreSQL 15.14 all require either an authenticated database session or a connection to the database service. enteliWEB's PostgreSQL instance listens only on 127.0.0.1 and is not reachable from the network.
- **Reporting engine XML handling is internal.**
  CVE-2020-13692 (PgJDBC, used by the BIRT reporting engine) requires attacker-controlled XML to reach the engine's XML handling. BIRT runs internally and its port can be restricted per the enteliWEB Hardening Guide.

CVE-2026-4800 (Lodash, React frontend) carries no backend code-execution exposure. Customers who have added custom frontend code calling _.template() with untrusted input should review that code path — this is the single finding where customer verification is recommended.

Across all 67 findings, no exploitation path exists against a standard enteliWEB deployment: the affected components are either absent, unreachable from the network, or reached only through a deprecated interface that is being removed.

Planned Remediation via Upgrade

The legacy SOAP interface is being removed entirely in enteliWEB 4.34. Each enteliWEB release also refreshes the bundled PHP runtime and PostgreSQL version; if a critical, exploitable CVE is identified in either, a patch will be issued within Delta Controls' defined SLA window. A full CVE-by-CVE technical assessment is available on request from the Delta Controls Cybersecurity Program.

Head Office
17850 56 Ave. Surrey
BC Canada V3S 1C7

Phone/Fax
Tel +1 604.574.9444
Fax +1 604.574.7630

Web /Email
info@deltacontrols.com
www.deltacontrols.com

Delta Intelligent Building Technologies

Appendix A: CVEs Reviewed

The following 67 CVEs from the customer-supplied scan were reviewed, grouped by the component they were raised against. CVE-2020-13692 and CVE-2026-6722 appear under two components in the source scan and are counted once here.

Component / Area	CVEs	CVE IDs
PHP	10	CVE-2026-7568, CVE-2026-7262, CVE-2026-7261, CVE-2026-6722, CVE-2026-7259, CVE-2026-7258, CVE-2025-14180, CVE-2025-14179, CVE-2025-14178, CVE-2025-14177
Python	3	CVE-2024-4030, CVE-2026-15308, CVE-2022-37454
XML parser	3	CVE-2024-45490, CVE-2023-52425, CVE-2023-27043
Frontend JavaScript (Lodash)	1	CVE-2026-4800
SQLite / enteliSKETCH	2	CVE-2026-11824, CVE-2026-11822
libcurl	1	CVE-2026-8927
phpseclib	1	CVE-2026-44167
PostgreSQL (incl. PgJDBC / BIRT)	16	CVE-2026-17543, CVE-2020-13692, CVE-2026-6637, CVE-2026-6479, CVE-2026-6478, CVE-2026-6477, CVE-2026-6475, CVE-2026-6474, CVE-2026-6473, CVE-2026-6472, CVE-2026-2006, CVE-2026-2005, CVE-2026-2004, CVE-2026-2003, CVE-2025-12818, CVE-2025-12817
zlib (documentation artifact)	1	CVE-2016-9840
Erlang / enteliVAULT	1	CVE-2026-42790
OS / unrelated component	1	CVE-2019-14822
OpenSSL	27	CVE-2026-9076, CVE-2026-7383, CVE-2026-45447, CVE-2026-45446, CVE-2026-45445, CVE-2026-42770, CVE-2026-42767, CVE-2026-42766, CVE-2026-34182, CVE-2026-34180, CVE-2026-31790, CVE-2026-31789, CVE-2026-28390, CVE-2026-28389, CVE-2026-28388, CVE-2026-28387, CVE-2026-22796, CVE-2026-22795, CVE-2025-9230, CVE-2025-69421, CVE-2025-69420, CVE-2025-69419, CVE-2025-69418, CVE-2025-68160, CVE-2025-15467, CVE-2024-9143, CVE-2024-13176
Total CVEs reviewed	67	—

Head Office
17850 56 Ave. Surrey
BC Canada V3S 1C7

Phone/Fax
Tel +1 604.574.9444
Fax +1 604.574.7630

Web /Email
info@deltacontrols.com
www.deltacontrols.com