PrivConvert

INDEPENDENT SECURITY ASSESSMENT

Security Assessment Report

Results of the security and integrity review conducted for the newly released 3D / mesh and geospatial file-conversion tools on the PrivConvert platform.

REPORT DATE	REPORT ID	SCOPE	CLASSIFICATION
12 July 2026	PC-SEC-2026-07	24 new conversion tools	Public

Human Review — ATTESTED

Reviewed and signed off by a member of the topriv security team. Findings and remediation were manually verified against live endpoints.

AI-Driven Testing — COMPLETED

Automated adversarial test suite executed by an AI security agent, covering malformed input, injection, resource-exhaustion and isolation scenarios.

01 Executive Summary

PrivConvert commissioned a combined human and AI-driven security assessment of a new set of file-conversion tools prior to and following their public release. The assessment focused on how the service handles hostile and malformed uploads, its resistance to injection and resource-exhaustion attacks, the strength of its processing isolation, and its data-privacy guarantees.

Result: No Critical or High-severity issues were identified. All tested tools correctly rejected hostile input, contained every attempted attack, and processed files entirely in volatile memory with no persistence. All tests passed.

24	0	0	100%
TOOLS ASSESSED	CRITICAL FINDINGS	HIGH FINDINGS	TESTS PASSED

02 Scope

The assessment covered the platform's newly introduced conversion tools:

- **3D & Mesh Conversions**
- **Geospatial Conversions**

18 tools converting between common 3D model formats used in printing, editing, scanning and web/AR workflows.

6 tools converting between common mapping and GPS data formats used in navigation, GIS and web mapping.

Testing was performed against the live production endpoints as well as the underlying conversion logic, using purpose-built malicious and malformed sample files.

03 Methodology

The assessment combined two independent layers of review:

- **Human security review (attested).** A security engineer reviewed the conversion logic and its trust boundaries, defined the threat model, and manually verified the outcome of each attack scenario against live endpoints.
- **AI-driven adversarial testing.** An AI security agent generated and executed a structured battery of attack payloads and integrity checks, confirming both correct conversion output and safe failure behaviour for every hostile case.

Each tool was evaluated for functional correctness (valid files convert accurately) and for safety (hostile files are rejected cleanly without impacting the service).

04 Test Coverage & Results

Area	What was tested	Result
Input validation	Corrupted, empty, truncated and wrong-type files disguised with valid extensions	**Pass**
Injection resistance	Hostile external-entity references, entity-expansion payloads, and script/markup injection via file content	**Pass**
Data exfiltration	Attempts to make the parser read local files or reach internal network resources	**Pass**
Resource exhaustion	Decompression ("zip") bombs, oversized inputs, and excessively complex/deeply-nested documents	**Pass**
Output integrity	Converted files re-validated with independent parsers to confirm faithful, uncorrupted results	**Pass**
Processing isolation	Confirmed untrusted parsing runs with no network access and cannot reach system files or credentials	**Pass**
Data privacy	Confirmed files are processed in memory only, never written to durable storage, and removed immediately after use	**Pass**
Service resilience	Service remained healthy and responsive throughout all attack scenarios	**Pass**

05 Findings Summary

Severity	Count	Notes
Critical	0	None identified.
High	0	None identified.
Medium	0	None identified.
Low	0	None identified.

06 Privacy Posture

Consistent with PrivConvert's privacy-first design, the assessment confirmed the following properties for the tools in scope:

- Uploaded files are processed entirely in volatile memory.
- No file content is written to durable storage during conversion.
- File data is discarded immediately once the converted result is delivered.
- Untrusted file parsing is isolated and has no access to the public internet.
- No account, sign-up or personal information is required to use the tools.

Attestation

This report confirms that the security assessment described above was carried out using both an independent AI-driven test suite and a human security review, and that no Critical or High-severity issues were outstanding at the time of publication.

HUMAN REVIEWER — ATTESTED
topriv Security Team

AI-DRIVEN TESTING — COMPLETED
Automated Security Agent