Service disruption on Monotype Foundry Platform (MFP) on 27 March 2026

Summary

On 27 March 2026 at 15:40 UTC, some users experienced intermittent errors and partial unavailability when using parts of the Monotype Foundry Platform (MFP). Most platform activity continued to operate normally, but a subset of requests did not complete successfully. Service was fully restored at 16:36 UTC, and the total duration was approximately 56 minutes. The disruption was caused by a high volume of automated internal security scan traffic that triggered protective request controls. No data loss or data corruption was observed.

Event Timeline (UTC)

- **Mar 27, 15:40 -** Monitoring detected intermittent errors and partial unavailability.
- **Mar 27, 15:49 -** Investigation began and the issue was reviewed by the operations team.
- **Mar 27, 16:01 -** Traffic protection settings were adjusted to allow normal platform requests while maintaining safeguards. Monitoring continued.
- **Mar 27, 16:36 -** Service was confirmed fully recovered and operating normally.

Root Cause Analysis

The disruption occurred when an internal security scan generated a higher-than-usual volume of automated requests from approved scanning sources. This traffic pattern exceeded protective request thresholds in the request handling layer, which is designed to protect the platform from abnormal request activity. As a result, a portion of legitimate platform requests between user-facing pages and backend service components was temporarily blocked, causing intermittent errors and partial unavailability for some users.

Key Observations

- Impact was limited to a subset of platform requests; many users continued to use MFP without interruption.
- The triggering traffic originated from an internal security scan rather than external malicious activity.
- Protective request controls operated as designed but were overly sensitive to this known internal traffic pattern.
- Service recovered after traffic controls were adjusted and platform stability was verified.
- No customer data was lost or corrupted during the event.

Corrective and Preventative Actions

Immediate Corrective Actions

- Adjusted protective request controls to permit legitimate platform requests while maintaining security safeguards.
- Monitored platform traffic and application health to confirm recovery and stability.

- Validated key user flows to confirm normal functionality had resumed.

Preventative Actions

- Coordinating the scheduling and scope of internal security scans to avoid peak usage periods.
- Tuning protection policies to better recognize and safely handle known internal scan patterns.
- Establishing controlled allowlisting for approved internal scanning sources while maintaining security guardrails.
- Enhancing monitoring and alerting to detect and isolate similar traffic patterns faster.

These measures ensure improved stability, resilience, and long-term scalability of Monotype services.