

Bitget

Incident Response Status Report

SEPTEMBER 28, 2026

Background

On September 25, 2026 (UTC+8), Bitget engaged Mandiant, part of Google Cloud, to respond to a suspected intrusion in their environment.

At 02:31 local time (UTC+8) on September 25, 2026, Bitget's security monitoring detected unauthorized outbound transfers from part of the exchange's hot and warm wallet infrastructure. Bitget estimated the loss in the range of US\$351.6 million and US\$387.5 million. The stolen assets span multiple blockchains and include XRP, ETH, USDT, USDC, BNB, AVAX, TRX, ZEC, Tether Gold (XAUt). Bitget did not observe evidence of private keys being compromised and its cold wallets were unaffected. Bitget's preliminary investigation indicates that the threat actor accessed a backend component of the wallet service. On-chain analysis revealed that the unauthorized transfers were executed alongside legitimate internal wallet operations on Ethereum until about 05:23 UTC+8 of the same day, almost three hours after detection.

Preliminary Findings

Forensic findings indicate that on September 24, 2026, a threat actor gained unauthorised privileged access to Bitget's third party security appliances A and B. The threat actor deployed a web shell onto the security appliance B and established a Command-and-Control (C2) connection.

Using the persistent access on security appliance B, the threat actor moved laterally to Bitget's production wallet job server and deployed malicious packages.

Mandiant's investigation is ongoing and based on the analysis completed thus far, the threat actor compromised network and security appliances and leveraged them to distribute malicious packages and gain control over the wallet job server.