

Dear GFC Group,

We refer to your incident notification concerning the unauthorised access to production systems and subsequent digital asset theft dated 11 January 2026.

Following our review of the submitted information, we note that, for the current submission, additional details are required to proceed with the assessment.

We kindly request that you provide the following information and supporting documentation:

1. Incident Description and Chronology

-Exact date and time of occurrence, detection, and containment

Response:

Incident summary:

Between 00:30 and 02:30 (UTC+0) unknown third parties gained unauthorized access to multiple production servers belonging to the company. As a result of this access, the attackers performed destructive actions, including deletion of data and disabling of critical services.

During the same timeframe, digital assets (including USDC, USDT, and BTC) were withdrawn without authorization via compromised API access to a third-party payment service. These withdrawals were not initiated or approved by the company.

The compromised assets originated from the company's payment processing server integrated with the Alphapo payment provider. The incident did not involve a direct hack of a blockchain wallet itself. Instead, the attacker gained unauthorized access to the payment server, from which they were able to execute illegitimate API requests to Alphapo. These API requests were used to initiate unauthorized withdrawals of cryptocurrency funds.

Based on the currently available information, the incident involved unauthorized access to the server infrastructure which allowed the attacker to obtain sensitive credentials and API keys used for communication with the payment provider.

Detection: 02:40 (UTC+0)

Containment:

Containment actions were initiated immediately after detection and included:

- isolation of affected servers

- initiation of full system reinstallation (reimage)
- revocation and rotation of API keys and credentials
- restriction of external access to affected systems

The payment provider Alphapo was contacted immediately after detection, and it was confirmed that unauthorized withdrawals had been executed through compromised API credentials.

Leaseweb hosting provider was also contacted to assist with access resets and infrastructure investigation.

The incident was reported to law enforcement on 12 January 2026.

-Detailed timeline of events

Replied above

-Method of detection (e.g. monitoring alert, third-party notification)

Automated monitoring alerts combined with internal operational alerts from the customer service team.

2. Systems, Data, and Services Affected

-Identification of affected systems, servers, and applications

Response:

Affected systems included:

- production game servers hosting casino applications
- database servers used for application data storage
- administrative back-office systems
- a payment processing server ("pay4play") integrated with the Alphapo cryptocurrency payment provider

-Confirmation of whether player personal data and/or game integrity were impacted

Response:

At this stage of the investigation, there is no evidence that player personal data or game integrity were compromised.

Number of affected players, accounts, and transactions

Response:

affected players: **0 (no player balances credited / no player funds stolen)**

number of unauthorized withdrawal transactions: **5**

3. Impact Assessment

-Quantified financial losses by asset type (USDC, USDT, BTC)

Response:

65,498.50453 USDC (allocated at USDC address: 0x9059Ab4C07d3bB0fC5a4E1B28271F7c44b9b4075)
1,853.839505 USDC (allocated at USDC address: 0x9059Ab4C07d3bB0fC5a4E1B28271F7c44b9b4075)
-19,438.88959234 USDTT + 333.92 USDTT(those funds were exchanged at HitBTC exchange
(support@hitbtc.com, legal@hitbtc.com) and later allocated at the same USDC address:
0x9059Ab4C07d3bB0fC5a4E1B28271F7c44b9b4075)
-0.14328483 BTC (allocated at BTC address: bc1qt6s78vfjrxuueqq843smu0sk8m25j0yp7zsac)

-Estimated number of impacted users

Response: 0

-Duration of the incident

Response:

The incident window is estimated to have occurred between approximately 00:30 and 02:30 (UTC+0), based on system monitoring and transaction timestamps.

-Assessment of legal, reputational, and player impact

Response:

Legal impact:

Police report filed and investigation ongoing.

Notification submitted to CGA.

Coordination ongoing with Leaseweb and the payment provider.

Reputational / player impact:

Short-term service interruption occurred.

No evidence of player data compromise.

Financial impact:

Unauthorized withdrawals of cryptocurrency assets as listed above.

Additional infrastructure recovery costs incurred.

4. Immediate Measures Taken

-Technical containment actions (e.g. server isolation, API key revocation)

Response:

- Isolated affected servers / initiated full OS reinstall (reimage)
- Disabled root password login, moved to SSH keys + IP allowlisting via VPN/bastion
- Reset/revoked API keys / rotated credentials for Alphapo and other integrations

-Safeguards implemented to prevent further unauthorized access

Response:

- Closed public ports; restricted port access to internal network only
- Implemented rate limits / withdrawal limits / approval workflow

-Details of any external cybersecurity or forensic experts engaged

Response:

- Engaged Leaseweb incident investigation

5. Root Cause and Remedial Actions

-Identified or suspected root cause of the incident

Response:

Preliminary b indicates that the incident resulted from unauthorized access to the server infrastructure which led to the exposure of sensitive credentials used for API communication with the payment provider. The exact intrusion vector remains under investigation.

-Description of the attack vector and vulnerabilities exploited

Response:

Based on the currently available information, the attackers obtained unauthorized access to the server infrastructure and were able to extract sensitive credentials used for API communication with the cryptocurrency payment provider.

These credentials were subsequently used to initiate unauthorized withdrawal requests via the payment provider API.

The exact technical intrusion vector remains under investigation. No evidence currently indicates compromise of the payment provider itself or of blockchain wallet infrastructure.

-Corrective actions already implemented

Response:

Migration to SSH key-based authentication only, implementation of IP allowlisting for administrative access, and full system reinstallation of affected servers.

Preventive measures planned, including timelines

Response:

Implementation of offsite backups

Introduction of centralized secrets management (vault)

Web application firewall (WAF) deployment and SQL injection hardening

Centralized logging/SIEM monitoring

Periodic access reviews and MFA for administrative systems

Progressive migration to a new platform architecture with enhanced security controls

6. Supporting Evidence (to be provided in original format)

- System, server, and API access logs
- Authentication and authorization logs
- Wallet and transaction logs, including full trace of unauthorized withdrawals
- Ledger extracts and reconciliation reports
- Incident response and forensic reports (if available)
- Backup and recovery logs
- Relevant internal policies and incident records

Response:

The following evidence has been preserved and can be provided upon request:

- Alphapo incident report confirming unauthorized withdrawals via API
- blockchain transaction records and transaction hashes for all unauthorized transfers
- internal incident summary prepared by the company's IT team
- hosting provider (Leaseweb) correspondence and incident tickets

7. Data Integrity Requirements

- Please ensure that all submitted evidence complies with the following:

- Data preserved in original, read-only format
- No alteration or filtering of logs
- SHA-256 hash values generated for each file
- Inclusion of an evidence manifest (file name, size, hash, timestamp)
- Maintenance of chain of custody records

Kindly submit the requested information and documentation.

Should you require any clarification regarding the above, please do not hesitate to contact us.

Response:

All available incident evidence has been preserved in its original form without modification.

Evidence files are stored in read-only format and may be accompanied by file metadata and hash verification if required.

The company maintains internal documentation of the incident investigation and evidence preservation process.