

BALGOPAL COMMERCIAL LIMITED

CIN: L43299MH1982PLC368610

Date: 11.05.2026

To,
The Department of Corporate Services,
BSE Limited,
Phiroze Jeejeebhoy Towers
Dalal Street, Mumbai- 400001

Scrip Code: 539834
Scrip Id: BALGOPAL

Subject: Announcement Under Regulation 30 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 for Balgopal Commercial Limited Disclosure of Cybersecurity Incident at Third-Party Service Provider.

Dear Sir/Madam,

Pursuant to Regulation 30 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, we wish to inform you that a cybersecurity incident has occurred at a third-party service provider engaged by the Company for hosting and managing its official email systems and website.

The said incident has resulted in disruption of the Company's email communication services and temporary unavailability of its website. In this regard, the Company has received a communication dated 11th May, 2026 from the said service provider informing that a critical zero-day vulnerability identified as CVE-2026-41940, affecting servers running the latest versions of cPanel/WHM, was disclosed by cPanel on 30 April 2026. As per the communication received, despite implementation of the recommended security updates and mitigation measures, the service provider's hosting infrastructure was subjected to a sophisticated cyberattack resulting in unauthorized access and severe damage to user data and services.

The service provider has further informed that the compromised server environment was no longer considered secure or trustworthy and, accordingly, all remaining recoverable data has been migrated to a new server environment. However, due to the nature and extent of the attack, certain data may only be partially recoverable or may not be recoverable at all. It was also informed that the attacker allegedly deleted the database server data as well as historical backup data from the compromised environment, thereby restricting restoration from backup sources.

ADDRESS: 901, 9th Floor, Crescent Royale, CTS No. 720 / 42-46, Oshiwara Village,
Andheri (West), Near VIP Plaza, Off New Link Road, Mumbai - 400053
Website: www.bcommercial.org/ **Email ID:** info@bcommercial.org
Contact: 9324922533

BALGOPAL COMMERCIAL LIMITED

CIN: L43299MH1982PLC368610

The Company would like to clarify that:

- The incident has occurred at the level of the external service provider and not within the Company's internal IT infrastructure.
- The Company is in continuous coordination with the service provider to assess the nature and extent of the incident.
- At this stage, the impact on the Company's data and operations is being evaluated.

As a precautionary measure:

- The Company's website has been temporarily taken offline.
- Email communications may be disrupted or unreliable.

Stakeholders are advised to exercise caution and verify any communication claiming to be from the Company during this period.

The service provider is currently undertaking restoration and remediation measures. The Company is also reviewing additional safeguards to mitigate such risks going forward.

The Company will keep the stock exchange informed of any further material developments in this regard.

A copy of the communication/email dated 11th May 2026 received from the concerned third-party service provider is enclosed herewith as Annexure - A for reference

This is for your information and record

Thanking You,
Yours faithfully,

For Balgopal Commercial Ltd

Ankit Ladha
Company Secretary & Compliance Officer
ICSI Membership No: A74941

ADDRESS: 901, 9th Floor, Crescent Royale, CTS No. 720 / 42-46, Oshiwara Village,
Andheri (West), Near VIP Plaza, Off New Link Road, Mumbai - 400053
Website: www.bcommercial.org/ **Email ID:** info@bcommercial.org
Contact: 9324922533

Security Incident and Server Migration Update



From Nisha Jain <jain.nishaa@gmail.com>
To <info@bcommercial.org>
Date 2026-05-11 12:33

From: Admin @ AapKaHost <admin@aapkahost.com>
Date: Wed, 11 May 2026 at 08:32
Subject: Security Incident and Server Migration Update
To: Nisha Jain <jain.nishaa@gmail.com>

We want to inform you of a recent cybersecurity incident that deeply impacted our hosting infrastructure.

cPanel/WHM recently disclosed a critical zero-day vulnerability CVE-2026-41940 affecting all servers running the latest versions of cPanel/WHM. According to the advisory issued by cPanel on 30 April 2026, this vulnerability could potentially allow unauthorized access to hosting control panels, resulting in modification or deletion of user data.

Immediately upon receiving the advisory, we implemented the required security updates and mitigation measures on our infrastructure. Despite these actions, our environment was subjected to a cyberattack. The attacker gained unauthorized access and severely damaged user data and services.

Our investigation indicated this was a sophisticated attack, and we identified multiple suspicious files on some user accounts that appeared to have been placed. As the old server environment was compromised and no longer trustworthy, we made the decision to migrate all remaining recoverable data to a new server.

At present:

- Due to the nature of the attack and the extent of data damage, some accounts may contain partial data, while others may have limited or no recoverable content.
- We are trying our best to recover the website from other alternative resources and upload within few weeks.

Unfortunately, the attacker completely deleted the database server data from the compromised environment. Additionally, historical backups were also removed by the attacker, which prevented restoration from those backup sets.