MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

November 2026

- AI-Detected Flaw Forces Websites Offline Worldwide
- Drones Strike Yandex Data Hub in Russia
- Cyberattack Hits French Supermarket Fridges
- Binance Hit by $6 Billion Crypto Hack
- Cyberattacks Target South Korea's Financial Sector
- Unrevoked Key Exposes LiteLLM Users to Cyberattacks
- Capcom Data Breach Affects 11.7 Million Accounts
- Cyberattack Disrupts US Federal Bankruptcy Court Operations
- India File



AI-Detected Flaw Forces Websites Offline Worldwide

Websites across the world experienced outages as operators rushed to secure their systems following the discovery of critical vulnerabilities in PHP, a widely used programming language.[1] The flaws, which had remained undetected for years, were identified using artificial intelligence (AI) , prompting PHP developers to release urgent security patches in October, 2026. Developers advised all users to update their software immediately to prevent potential exploitation.

PHP, which stands for Hypertext Preprocessor, is an open-source, server-side programming language used to build dynamic websites and web applications.[2] Developed in the early 1990s, it runs on web servers and processes requests to deliver content to users. Despite being several decades old, PHP remains widely used and supports numerous platforms, including Wikipedia, e-commerce websites and WordPress, the content management system that powers a large proportion of websites worldwide.

Drones Strike Yandex Data Hub in Russia

Drones struck a data centre operated by Yandex, Russia's leading AI and technology company, marking the first major attack on a Russian data hub since the outbreak of the war with Ukraine.[3] The company confirmed that the strike triggered a fire at one of its five major data centres, which houses tens of thousands of servers, forcing it to suspend operations at the facility. Yandex said it was working to restore the affected services. Although the company maintained that its core consumer services remained unaffected, it did not disclose the full extent of the damage.

Often referred to as "Russia's Google", Yandex launched the country's first search engine in 1997. Today, its portfolio includes YandexGPT, one of Russia's leading AI models, cloud computing services, and popular consumer platforms such as Yandex Taxi and Yandex Music.

Cyberattack Hits French Supermarket Fridges

Hundreds of supermarkets across France were affected by a cyberattack that disrupted their refrigeration systems, causing fridges and freezers to heat up and resulting in the spoilage of fresh and frozen food worth an estimated millions of euros.[4] According to one of the affected supermarket chains, hackers compromised the software used to regulate refrigeration temperatures, remotely forcing some units to reach as high as 50°C (120°F) overnight.

The software, developed to help retailers monitor and manage refrigeration units remotely, was allegedly manipulated by the attackers to override normal temperature settings. Supermarket freezers typically undergo a brief overnight defrosting cycle, during which temperatures rise slightly before returning to normal. However, in this incident, the attackers reportedly forced the units to remain heated for an extended period. Danfoss, the company associated with the refrigeration technology, did not confirm reports about the maximum temperatures reached by the affected units.

Binance Hit by $6 Billion Crypto Hack

Binance, the world's largest cryptocurrency exchange by trading volume, suffered a major cyberattack that resulted in the theft of assets estimated at approximately $6.3 billion, potentially making it the largest crypto-related hack on record.[5] According to the company's assessment, around $3 billion of the stolen assets have since been frozen, including approximately $2.3 billion in USDT and USDC stablecoins. The freezing was carried out by the respective token issuers, who blocked transactions involving the affected blockchain addresses, preventing the attacker from transferring or converting those funds. According to the company's statement, the attack may have originated from an engineer's compromised laptop, which could have provided the attackers with unauthorised access to its systems.

Cyberattacks Target South Korea's Financial Sector

South Korea's financial sector has faced another wave of cyberattacks, raising concerns about the growing threat of AI-driven hacking across Asia.[6] The latest incidents have targeted brokerage firms Daishin Securities and Mirae Asset Global Investments, along with cryptocurrency exchange Bithumb. According to reports, Daishin Securities disclosed a data breach involving the personal information of 38,490 customers, including their names, email addresses and mobile phone numbers.

In response to the growing number of cyber incidents targeting financial institutions and government agencies, South Korea's financial regulator has called for stronger cybersecurity measures. The government also plans to conduct security assessments of dozens of private-sector IT systems to identify vulnerabilities and strengthen digital defences.

Unrevoked Key Exposes LiteLLM Users to Cyberattacks

LiteLLM, an open-source tool widely used by AI developers, confirmed that a supply-chain attack affecting potentially tens of thousands of users originated from an accidentally exposed security key.[7] According to the company's root-cause analysis, the incident stemmed from the earlier accidental publication of a configuration file containing the master key for an internal tool used to manage AI agents. Although LiteLLM detected and removed the exposed file at the time, it failed to revoke the compromised key. An unidentified attacker later used it to gain access to the company's internal tools and obtain a token that provided control over its GitHub repositories. The attacker then bypassed multiple security controls to distribute a compromised version of LiteLLM containing malware designed to steal users' credentials.

Capcom Data Breach Affects 11.7 Million Accounts

Japanese video game company Capcom has reported a cyberattack on its online account system, potentially exposing email addresses and IP addresses linked to 11.7 million user accounts worldwide.[8] The breach targeted Capcom ID, the account

platform used to access the company's digital store and online games.

The investigation also found evidence that attackers accessed additional personal information, including dates of birth, gender, country or region, and nicknames, associated with 43 accounts. Capcom detected suspicious activity on 19 October and subsequently launched an investigation, introducing emergency measures to secure its IT systems. While the source of the breach remains unclear, the company has warned affected users to remain alert to phishing emails and messages impersonating Capcom.

Cyberattack Disrupts US Federal Bankruptcy Court Operations

Several online services supporting the US federal bankruptcy court system were taken offline following a cybersecurity incident involving a third-party contractor, the Administrative Office of the US Courts (AOC) confirmed.[9] BAE Systems Inc., the US subsidiary of British defence contractor BAE Systems, operates the systems and websites of the Bankruptcy Noticing Center (BNC) on behalf of the federal judiciary. According to the AOC, access to all BNC systems and websites managed by BAE Systems were suspended, disrupting the associated bankruptcy notification process. The BNC is responsible for generating and distributing bankruptcy notices on behalf of federal bankruptcy courts across the United States.

India File

- The State Bank of India (SBI) reported a cyber incident involving the suspected exposure of 3,897 customer records containing personally identifiable information (PII) on the dark web.[10] The bank stated that the incident had no material impact on its core operations, financial performance or business continuity. A preliminary analysis of approximately 3.75 lakh records identified 3,897 records containing personal information. The exposed data reportedly included customers' names, registered mobile numbers, dates of birth, gender, email addresses and residential addresses.
- India's cybersecurity agency, CERT-In, has confirmed that AI models undergoing testing managed to breach the live systems of Indian organisations and access confidential records without detection.[11] This marks the country's first official acknowledgement of such an incident, amid growing reports of similar unauthorised activities by AI agents worldwide. According to CERT-In, AI model providers voluntarily reported that their agents had exceeded the permissions assigned to them during test runs, gaining unauthorised access to data held by Indian companies, including sensitive business records.
- As part of the broader India–Sri Lanka bilateral partnership on digitalisation and cooperation in emerging technologies, including AI, an Indian delegation comprising Dr Sanjay Bahl, Director General of CERT-In, and Mr Amit Shukla, Joint Secretary (Cyber Diplomacy) at the Ministry of External Affairs, visited Colombo for the first round of bilateral cyber consultations.[12]

During the visit, the delegation met Eranga Weeraratne, Deputy Minister of Digital Economy, to discuss cybersecurity governance frameworks and emerging AI-related cybersecurity challenges. The discussions also focused on strengthening cooperation through the exchange of cyber threat assessments, sharing CERT-In's best practices, and enhancing collaboration in capacity building and cyber incident response.

- A major data breach has affected the entertainment industry, exposing confidential records associated with more than 500 film titles through the digital portal of India's Central Board of Film Certification (CBFC).[13] The leaked documents reportedly included film scripts, details of cuts and modifications mandated by the censor board, and agreements disclosing the amounts paid by distributors to acquire film release rights in India. While most of the affected titles were feature films, the breach did not involve the films themselves.
- India and Singapore have signed a Memorandum of Understanding (MoU) to strengthen bilateral cooperation in cybersecurity, with a focus on information sharing and coordinated responses to cyber incidents.[14] The agreement seeks to enhance collaboration between the two countries' national computer emergency response teams to improve their cyber resilience. The MoU brings together Singapore's Cyber Emergency Response Team (SingCERT), operating under the Cyber Security Agency (CSA), and CERT-In, under the Ministry of Electronics and Information Technology (MeitY). It was exchanged on the sidelines of Singapore International Cyber Week 2026 and provides a framework for closer cooperation between the two agencies in addressing emerging cyber threats and responding to incidents.
- Prime Minister Narendra Modi inaugurated the Reserve Bank of India's (RBI) newly established Data Centre and Cybersecurity Training Institute in Bhubaneswar, Odisha.[15] He highlighted the significance of the facilities for strengthening the country's digital and cybersecurity infrastructure, noting that they would benefit both Odisha and the nation. The Prime Minister also described the inauguration as reflecting a broader shift in India's approach to governance, with greater emphasis on development, expanding the scale of public services and ensuring their effective delivery to citizens.

[1] Reuters, Government websites go dark after AI-discovered flaw sparks security scramble, 21 October 2026, https://www.reuters.com/world/asia-pacific/eu-agency-warns-websites-may-need-be-taken-offline-php-prepares-patches-2026-10-21/

[2] BBC, What is PHP and why did it spark a global cyber-security scramble?, 23 October 2026, https://www.bbc.com/news/articles/c3qjnwye0ep5o

[3] Reuters, Drones hit Yandex site in first major attack on Russian data hub, 8 October 2026, https://www.reuters.com/world/drones-hit-yandex-data-centre-first-major-attack-russian-data-hub-2026-10-08/

[4] BBC, Fridges in French supermarkets hit by cyber attack, 12 October 2026, https://www.bbc.com/news/articles/crq5nzxv9q4yo

[5] CoinDesk, Binance loses over $6 billion in 'biggest crypto hack in history', 30 October 2026, https://www.coindesk.com/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets

[6] TechCrunch, South Korea's financial industry hit by fresh wave of cyberattacks, 28 October 2026, https://techcrunch.com/2026/10/28/south-koreas-financial-industry-hit-by-fresh-wave-of-cyberattacks/

[7] The Record, Popular AI tool LiteLLM says unrevoked key allowed hackers to target users, 26 October 2026, https://therecord.media/litellm-hackers-ai-malware

[8] PCMag, Capcom Suffers a Breach Affecting 11.7 Million Accounts, 22 October 2026, https://www.pcmag.com/news/capcom-suffers-a-breach-affecting-117-million-accounts

[9] Reuters, US federal bankruptcy court operations disrupted by cybersecurity incident, 16 October 2026, https://www.reuters.com/legal/litigation/us-federal-bankruptcy-court-operations-disrupted-by-cybersecurity-incident-2026-10-16/

[10] India Today, SBI confirms cyberattack, 3,897 customer records stolen and put on dark web, 21 October 2026, https://www.indiatoday.in/technology/news/story/sbi-confirms-cyberattack-3897-customer-records-stolen-and-put-on-dark-web-3021725-2026-10-21

[11] Reuters, Rogue AI agents broke into Indian firms' live systems, government says, 16 October 2026, https://www.reuters.com/legal/litigation/rogue-ai-agents-broke-into-indian-firms-live-systems-government-says-2026-10-16/

[12] Sri Lanka Mirror, India - Sri Lanka hold consultations on cyber-security, 6 October 2026, https://srilankamirror.com/2026/10/06/news/india-sri-lanka-hold-consultations-on-cyber-security

[13] The Print, CBFC data breach exposes scripts, censor cuts, film distribution deals for over 500 titles, 26 October 2026, https://theprint.in/entertainment/cbfc-data-breach-scripts-censor-cuts-film-distribution/3081894/

[14] CRN, Singapore, India formalise cybersecurity cooperation on incident response and threat information sharing, 15 October 2026, https://www.crnasia.com/india/news/2026/singapore-india-formalise-cybersecurity-cooperation-on-incident-response-and-threat-information-sharing

[15] PIB, Prime Minister Shri Narendra Modi inaugurates RBI's newly established Data Centre and Cybersecurity Training Institute in Bhubaneswar, Odisha, 25 October 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2328250&reg=48&lang=2