

Critical **PHP** bugs put websites and servers at a grave risk

GOOGLE, OPENAI DEPLOY AI TOOLS TO IDENTIFY AND ANALYSE FLAWS

NEW DELHI

GLOBAL technology giants, cybersecurity researchers and government agencies have launched a coordinated response following the discovery of two critical vulnerabilities in PHP.

The widely used open-source programming language powers a large share of websites and web applications worldwide.

The vulnerabilities, collectively dubbed 'PHP2Shell' could allow attackers to remotely execute malicious code on affected servers, potentially giving them access to sensitive files, databases and other critical systems, according to security researchers involved in the disclosure.

The findings have triggered concern across the cybersecurity community because of PHP's extensive use in websites, enterprise applications and online services, raising fears that successful exploitation could affect a significant number of internet-facing



The observations indicate that threat actors may have been aware of the vulnerabilities prior to their public disclosure. It remains unclear how attackers may have obtained information about the flaws in advance

systems. Regarding this, tech giant Amazon has said that its threat intelligence team identified attempts to exploit the vulnerabilities before details were made public. The company used its MadPot threat detection network, which monitors suspicious activity across internet-con-

nected infrastructure, to spot signs of malicious activity targeting the flaws.

The observations indicate that threat actors may have been aware of the vulnerabilities prior to their public disclosure. It remains unclear how attackers may have obtained information about the flaws in advance, according to Amazon.

The incident has also highlighted the growing role of artificial intelligence in cybersecurity research.

Another major technology firm Google said its cloud security unit, Wiz, used AI-powered systems to assist in identifying and analysing the vulnerabilities.

The company added that its Gemini AI models were deployed to evaluate potential attack scenarios, assess the impact of the flaws and help validate security patches developed to address the risks.

"PHP and Wiz Research disclosed two critical vulnerabilities in the core PHP language runtime that can expose applications to unauthenticated remote code execution and memory disclosure. Wiz used a mix of models to identify and help remediate these vulnerabilities," Google said. Meanwhile, OpenAI said researchers working alongside its artificial intelligence models helped discover and investigate the vulnerabilities.

The AI giant firm said it spent the past two months coordinating a coalition of software maintainers, security vendors and cybersecurity specialists to prepare fixes and mitigation measures before public disclosure.



Centre cautions TV channels over AI and code violations

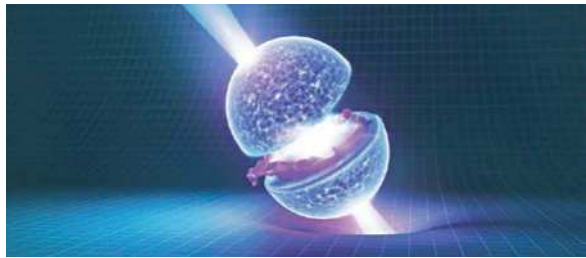
NEW DELHI

NEW DELHI: The Ministry of Information and Broadcasting (I&B) on Wednesday advised private satellite television channels to strictly comply with the Programme Code and exercise caution while using artificial intelligence tools in news and programme production, warning that violations could attract regulatory action.

In an advisory, the ministry said several channels had violated provisions of the Programme Code prescribed under the Cable Television Networks (Regulation) Act, 1995, and the Cable Television Networks Rules, 1994. It cautioned that any breach of the code could invite action under the existing regulatory framework. "The use of AI tools may be limited to assistive capacity without compromising the accuracy, authenticity or sensitivity of news content," it said. The ministry also raised concerns over the growing use of artificial intelligence technologies in broadcasting and asked channels to exercise due caution while deploying AI tools, including generative AI, for graphics, virtual news presentations and other programming.

Indian scientists reveal how neutron star feeds on cosmic matter

FINDINGS EXPLAIN VARIATIONS IN SECONDARY X-RAY EMISSION LINES



INDIAN scientists have discovered that one of the brightest X ray pulsars, Centaurus X 3, is gobbling up material through an accretion disk — a rare behaviour for pulsars of its kind, an official statement said. The finding was made by researchers at the Raman Research Institute (RRI), an autonomous institution of the Department of Science and Technology (DST), led by Kinjal Roy.

The study has implications in developing better-informed models of the system, which is one of the most widely studied binary pulsars that has drawn the attention of scientists because of its intense brightness.

Further, it will lead to enhanced understanding of binary pulsars in general.

An X-ray binary pulsar consists of a pulsar—a highly magnetised neutron star, and a Sun-like star bound in a gravitational dance. A neutron star is a celestial body with the mass of our sun crunched into a ball the size of Bangalore. "In an X-ray binary, the pulsar's extreme gravity pulls in

material ejected by its companion star, and the pulsar starts accreting material from it, shooting out X-rays in the process," the statement from the Ministry of Science & Technology said.

Centaurus X-3, a high-mass X-ray binary (HMXB) where the companion is more than 10 times the Sun's mass, was one of the first X-ray pulsars to be discovered, and the third X-ray source to be discovered in the constellation Centaurus, 24,000 light years away.

Pulsars emit radiation from their magnetic poles, known as the primary emission. As the pulsar spins, this radiation sweeps past any satellite waiting to detect it. This radiation also falls around the neutron star.

Structures in its wider environment absorb and re-emit

this radiation, dubbed as the secondary radiation.

These structures help understand the system's physical parameters, such as its orientation and magnetic field strength, leading to enhanced understanding of binary pulsars, the statement noted.

Scientists from the Raman Research Institute (RRI) investigated four secondary emission lines in depth and found that the structure responsible for the varying lines must be co-rotating with the pulsar. Detection revealed an accretion stream, which is a structure that channels material from the accretion disk towards the pulsar, that is causing the variability in the secondary emission lines.

An accretion stream proved the existence of an accretion disk, the ministry said.

MeitY launches probe into eMudhra certificate incident

CERT-In issues advisory outlining mitigation measures

NEW DELHI

THE Ministry of Electronics and Information Technology (MeitY) has launched an investigation into a security incident involving eMudhra, while the Indian Computer Emergency Response Team (CERT-In) has issued an advisory outlining mitigation measures.

The impact on Indian websites and applications was limited and temporary, government sources said cited by NDTV Profit, adding that eMudhra's India-regulated Digital Signature Certificate (DSC) and eSign services were not affected. Officials also cautioned against exaggerated claims circulating on social media and said more details would be shared after the investigation is completed.

"We are taking it up with them, and we are also taking it up with other operators to check whether they have further issues," as per the report.

According to eMudhra, the issue relates to a small segment of its international



Transport Layer Security (TLS) certificate business and does not involve its domestic digital signature operations.

The company stated that a flaw in its system resulted in the creation of weak cryptographic keys alongside the intended strong keys.

The issue came to light after a researcher alerted major technology firms, including Apple, Google, Microsoft and Mozilla, that the weak keys could potentially be reverse-engineered, including through AI-assisted techniques.

In its advisory, CERT-In said eMudhra had reported the compromise of private keys associated with eight intermediate certification authority certificates within its public key infrastructure

(PKI), including six TLS certificates and two code-signing certificates.

TLS certificates are used to secure communications between websites, browsers and applications.

Security experts warn that misuse of compromised keys could enable attackers to issue fraudulent certificates for domains they do not control, impersonate legitimate websites and potentially intercept or alter encrypted communications. Similarly, compromised code-signing certificates could be misused to distribute software appearing to come from trusted sources.

eMudhra maintained that its infrastructure had not been breached and that no customer data had been compromised.

India's aerospace industry likely to grow twice as fast as global market

NEW DELHI

INDIA's aerospace industry is expected to grow twice at the pace of the global market, driven by state backed reforms, rising private capital and closer collaboration with the Indian Space Research Organisation (ISRO), a new report has said.

The report from Forbes cited Arkam Ventures as saying that the sector is currently valued at \$13 billion and is forecast to over triple



to \$40 billion by 2030, with some estimates projecting a \$44 billion space economy by 2033.

"To win the celestial race, India's space startups need to strongly leverage the nation's unique attributes in software development to cater to the downstream market of data

mining from satellites," the report said.

Private firms are expected to participate in up to 45 launches a year for international customers by 2030 and to manufacture one third of the world's earth observation satellites, it added.

India is also likely to emerge as a major exporter of avionics, Global Navigation Satellite System (GNSS), Satellite Communication (SATCOM) and ground Radio Frequency (RF) systems.

US approves new Hepatitis B treatment

WASHINGTON

THE United States has approved a new treatment for chronic hepatitis B that could allow some patients to stop taking antiviral medicines while maintaining control over the virus.

The US Food and Drug Administration (FDA) announced Tuesday that it had approved Hibsago (bepirovirsen), an injectable medicine developed by GSK, for certain adults with chronic hepatitis B who do not have

cirrhosis. The treatment is the first FDA-approved antisense oligonucleotide for hepatitis B, using a technology designed to interfere with the genetic instructions that allow the virus to reproduce and produce viral proteins.

The new approach offers some eligible patients the possibility of maintaining viral control after stopping all hepatitis B therapy.

"For many people living with chronic hepatitis B, treatment can mean taking antiviral medication for years



to keep the virus suppressed," said Wendy Carter, acting director of the FDA's Office of Infectious Diseases.

"Hibsago provides a new treatment approach that gives some patients the

possibility of maintaining control of the virus after all chronic HBV treatment has ended. This approval represents an important advance for people living with this serious disease," she said.

The approval applies to adults without cirrhosis who have received antiviral therapy for at least six months and have suppressed levels of hepatitis B virus in their blood.

Patients must also have hepatitis B surface antigen levels of 3,000 international

units per millilitre or less, established through an FDA-authorised diagnostic test.

The FDA said the treatment was evaluated in two clinical trials comparing Hibsago with a placebo.

Patients received injections under the skin for up to 24 weeks while continuing their existing antiviral medication.

They were required to remain on their regular antiviral treatment for at least another 24 weeks after the final Hibsago injection.



THE POLITICA

Nothing political about it

DEEPIKA BHAN

WHEN American singer Mary Millben made an explosive claim about the Delhi protests, alleging that the Cockroach Janata Party (CJP) was being funded by "select US donors", it did not come entirely as a surprise to those who had already been questioning the source of money behind the protests.

Questions have been raised for some time about the funding of these activities. The scale of the arrangements at some protests has also drawn attention. From frequent air travel and expensive cars to food, ice cream, cakes and drinks being served in abundance during the July Janatar Mantar protest, the expenditure appeared substantial. At one point, the crowds being served numbered in the hundreds. There have also been reports of parties at expensive hotels.

All this raises a basic question: who is paying for these activities, and where is the money coming from?

The CJP maintains that it is self-funded by its founding team and does not accept political donations. Its founder, Abhijeet Dipke, has faced questions about

Protests are loud, but where is the money coming from?

CJP maintains that it is self-funded by its founding team and does not accept political donations

the funding. At a press meet in Mumbai on October 1, he dismissed the relevance of such queries, asking what disclosing the funding would have to do with alleged irregularities in the Election Commission.

He also declared that he wore shoes worth Rs30,000 and was not ashamed of it because he could afford them.

There is nothing wrong with wearing expensive shoes if one can afford them. But that is not the point. Personal spending and financing an organisation are two different matters. The question is not about the price of Dipke's shoes, but about the money being spent on organising protests and running political campaigns.

If the funding is transparent, a clear explanation should help settle the matter. An aggressive response or a counter-question does not answer it. Questions about money should not automatically be seen as an attempt to silence dissent.

Millben's remarks have added another dimension to this debate. She is not an elected politician, but an American singer and actor who has performed for five US presidents -- George W Bush, Barack Obama, Donald Trump dur-

ing his first term, Joe Biden, and Trump during his second term.

In a video message addressed to young Indians, she named billionaire George Soros, alleging that he and his network were funding protests across the world, particularly in countries led by conservative leaders.

"It's the same person or same group of people, certainly coming from America, that's funding a lot of these protests across the world, particularly when you have a conservative leader at the top of the ticket or running the government. The name is George Soros, and that whole machine of people are constantly funding a lot of these protests and chaos that's breaking out across the world," she said.

Millben, however, has not provided evidence to substantiate this allegation. In an earlier post on X, she described what she believed was a pattern followed by certain US-based donors: targeting conservative leaders, identifying educated people from those countries, radicalising them and funding activities that create chaos.

The CJP was quick to hit back. But the larger question remains. Are protest movements receiv-



If the funding is transparent, a clear explanation should help settle the matter. An aggressive response or a counter-question does not answer it. Questions about money should not automatically be seen as an attempt to silence dissent

ing money from sources that are not being disclosed? If so, is that funding lawful, and are the relevant rules being followed?

Senior advocate and former Solicitor General of India Harish Salve has also raised concerns about foreign funding and external interference. In an interview with IANS, he alleged that some foreign countries, particularly the United States, were unhappy with India and suggested that develop-

ments in Nepal, Sri Lanka and Bangladesh pointed to a pattern of external interference.

"I believe that foreign funding is being provided for these efforts and that they are being instigated from abroad. This is my allegation. Some foreign countries, particularly the United States, are not happy with India," Salve said.

He also questioned the funding of protest activities, referring to YouTubers, Dipke, Saurav

Das and people living overseas. Organising protests, he argued, required money, and the source of that money needed to be examined.

These are serious allegations. They should neither be accepted as facts nor dismissed without examination. If there is evidence of unlawful foreign funding or external interference, the government must investigate it.

The protests are taking place at a difficult time for India. The US-Israel attack on Iran and the closure of the Strait of Hormuz have created major economic and strategic challenges. The government has had to deal with the international fallout while attempting to protect the country from its economic consequences. Despite the uncertainties created by US President Donald Trump's unpredictable policies, India has continued to pursue economic partnerships with other countries and protect its strategic interests.

At such a time, a battle is being fought with the government through social media narratives, protests and confrontations with the police. A few reels of protesters shouting slogans, clashing with police personnel or using abusive language against

the Prime Minister may attract millions of views. But online attention is not the same as public support.

India has an electoral system in which governments can be challenged and changed through votes. That is the test which political parties and movements ultimately have to face. Opposing the government is a basic democratic right. Peaceful protests are an essential part of democracy. But the right to protest does not place any organisation beyond questions about its finances. The CJP and other groups should answer legitimate questions about their funding.

Attempts to build narratives and generate chaos may grab headlines and attract attention on social media, but they cannot by themselves bring about regime change in India. More than those who may be operating from foreign countries to influence opinion here, it is those who take the money and carry out such activities who must answer questions.

If any wrongdoing is established, those responsible should be held accountable. Dissent is a democratic right, but it cannot become a licence to mislead. (IANS)