

Global Threat Intelligence Report

Featuring AI Driven Threats and Cyber Resilience

Volume 19 - November 2026

KDDI Europe

KDDI America

Table of Contents

This Month at a Glance 3

NEWS 4
CenterPoint Energy Data Breach [1] 4
Burger King Japan suffers data breach [2] 4

THREAT INSIGHTS 5

The Help Desk Messaging You Might Not Work There. 5

REGULATORY INSIGHTS 8

PHP2Shell: A Global Test of Vulnerability Governance 8

Response from UK, EU, US and Japan 8

Evidence of Exploitation and Reporting Limitations 10

Governance and Assurance Priorities 10

Conclusion 11

TECHNOLOGY INSIGHTS 12

Qilin by the Numbers 13

Engagements with Law Enforcement 13

Ransomware Characteristics 13

What Makes Qilin Stand Out from Other Hacker Groups? 14

Qilin's Operation 15

Analysing Attack Patterns: 2 Examples 16

Overall Suggestions 17

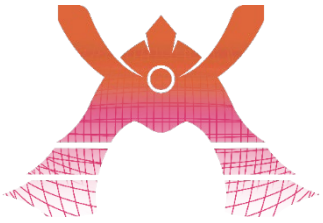
SUGGESTIONS 18

Protection, Prevention and Takeaways 18

COMMON VULNERABILITIES AND EXPOSURES (CVES) 19

REFERENCES 20

Introduction



Welcome to the Global Threat Intelligence Report. This report provides a concise overview of recent cybersecurity threats, industry developments, and regulatory changes that may impact organisations worldwide.

At KDDI Europe, we remain committed to helping customers strengthen their cyber resilience through security expertise, continuous monitoring, and proactive threat intelligence. We hope the insights in this report support informed decision-making and stronger security outcomes.

With the addition of KDDI America's insights, the report now draws on expertise from across the KDDI Group, providing a broader perspective on emerging cyber threats and trends.

This Month at a Glance

This month, we examine the CenterPoint Energy and Burger King Japan breaches, IT support impersonation through Microsoft Teams, and Qilin ransomware. Our PHP2Shell analysis explores vulnerability governance and responses across the UK, EU, US and Japan. Key priorities include securing identities, reducing exposure, protecting data and testing detection, response and recovery.

Disclaimer

This content is provided for general informational purposes only and does not constitute legal advice. Readers should seek guidance from qualified legal professionals regarding the application of any law or regulation to their specific circumstances.

News

The Latest Cybersecurity news



Henry Finnah
Cyber Security Service Development Engineer

CenterPoint Energy Data Breach [1]

On 14 October 2026, A regulatory disclosure confirmed that 1,062,060 Texas residents were affected by a data breach involving customer information. The compromised data included names, addresses, Social Security information and driver's licence numbers.

The incident had initially been disclosed in September after an unauthorised third party claimed to possess customer information. The breach highlights the continuing risks associated with externally accessible systems and the large volumes of sensitive personal information held by critical infrastructure providers.

Importantly, CenterPoint reported that its electricity and natural-gas services remained operational, with no disruption to energy delivery resulting from the cyber incident.

Burger King Japan suffers data breach [2]

On 15 October 2026, Burger King Japan disclosed unauthorised access to its smartphone-app membership environment, potentially exposing approximately 11.18 million customer records.

Compromised information included names, email addresses, telephone numbers, dates of birth and other customer profile information. Credit-card details were not stored within the affected system, while password exposure had not been confirmed.

The scale of the incident makes it a significant consumer-data breach and demonstrates the potential impact of attacks targeting customer loyalty and mobile application platforms containing large repositories of personally identifiable information.

Threat Insights



Hamza Bashir
Cyber Security Pre-Sales Consultant

The Help Desk Messaging You Might Not Work There.

Attackers have found a quieter door than email. It is sitting in your Microsoft Teams, and for most companies it is wide open.

It starts with your inbox melting. In the space of a few minutes, hundreds of newsletter sign-ups and subscription confirmations pour in, burying everything real under junk. You are annoyed and a little alarmed. Then, right on cue, a message arrives in Microsoft Teams from "IT Support (Internal)", offering to sort it out for you. [3]

They are not from your IT department. They are not even from your company. And if you let them help, they will be inside your network in under fifteen minutes. [3]

This is the technique security firm Arctic Wolf pulled apart after studying more than 400 incidents of it, and it deserves attention for one simple reason: it sidesteps almost everything companies have spent years teaching staff to watch for. [4]

Why Teams, and why now

For a decade, the security awareness message has been about email. Check the sender, hover over links, do not open strange attachments. People have slowly got better at it. So attackers moved to the channel nobody polices with the same suspicion.

The quiet problem is that Microsoft Teams lets people from outside your company message your staff by default. This is called external access, or federation, and in some organisations it is switched on and forgotten. [3]An attacker spins up their own Teams tenant, often a free one with a throwaway address Microsoft never verifies, and can message your employees directly. Roughly a third of the cases Arctic Wolf saw used exactly these default, unverified tenants. [3]

So the message does not land in the quarantined, scanned, treated-with-suspicion world of email. It arrives in Teams, the place your colleagues talk to each other all day. That change of scenery does most of the attacker's work for them.

The con itself

The inbox flood at the start is not the attack. It is the setup. It manufactures a problem, and a moment of panic, so that the "IT Support" message offering to fix it feels like a relief rather than a red flag. [3]

From there it is a confidence trick with a clear goal: get the victim to install a remote-control tool. Usually it is Quick Assist, a legitimate program already built into Windows, which makes it feel safe. The attacker reads out a six-digit code, the victim types it in, and the stranger now has hands-on control of the machine. [3]Other tools get used too, from AnyDesk to TeamViewer, and once in, the attackers often quietly install a second one so they still have a way back if the first is spotted. [3]

What follows is the familiar damage: harvesting credentials, spreading to other machines, and in a number of cases ending in ransomware, with crews like Black Basta, Cactus and Chaos linked to the method. [3]Arctic Wolf watched attackers hit several employees inside a single company within about five minutes, working through a list. [3]

There are fingerprints of industrial scale, too. The crews keep links out of the chat entirely, which quietly dodges the Safe Links scanning that would flag a bad URL, and Arctic Wolf found emoji peppered through more than a hundred of the fake "IT Support" names, a quirk it suspects points to AI writing the messages. [5]

Why this one is worth your attention

Three things make this more than another phishing variant.

First, there is nothing to patch. No vulnerability, no exploit, no malware in the opening move. The "way in" is a trusted app, a legitimate remote-access tool, and an employee trying to be helpful. Your technical defences are not being beaten, they are being walked around.

Second, the trust is misplaced by design. An email from outside at least looks like it is from outside. A Teams message feels internal, even when it is not, and the small "External" tag that would give it away is easy to miss when you are flustered and your inbox is on fire.

Third, and this is the fixable part, most companies have simply never closed the door. Teams external access is on by default, so unless someone has deliberately restricted it to a short list of trusted partners, your staff can be messaged by anyone who sets up a tenant. That is a setting, not a budget line, and it shuts a lot of this down on its own. [3]

What actually helps

The prevention is unglamorous and mostly free: lock Teams external chat down to domains you actually work with, pull back or remove Quick Assist, and block remote-access tools your own IT did not install. [3]Add a simple rule everyone understands, that real IT will never message you out of the blue in Teams and talk you through installing something, verified by a call back to a number you already know. [3]

But prevention will not catch every case, because the whole method is built to look legitimate. The thing that decides how one of these ends is whether anyone notices the next step: a remote-access tool appearing on a machine, followed minutes later by that machine quietly querying Active Directory for a list of every user and computer. [3]A real employee does not do that. Spotting that behaviour quickly, and acting on it before the five-minute sweep becomes a ransomware incident, is the difference between a blocked attempt and a bad month. That is continuous detection, not a cleverer wall.

The Bottom Line

The attackers have not got smarter, they have just changed rooms. They left the inbox, where everyone is watching, for the chat window, where almost nobody is. The question for your organisation is not whether your email filtering is good. It is whether a stranger can message your staff in Teams at all, and whether anyone would notice the "helpful" session that follows.

Regulatory Insights



Shintaro Takeda
Regional Chief Information Security Officer

PHP2Shell: A Global Test of Vulnerability Governance

A cross-border case study of how a widely embedded software vulnerability became a governance, assurance and regulatory challenge.

On 21 October 2026, the PHP project released security updates for two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619, collectively known as PHP2Shell. [6] [7] Successful exploitation could allow an unauthenticated attacker to execute code remotely through an affected PHP worker process. [6] [7] Affected environments include PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. [6] [7] Exploitability varies by version, configuration and runtime conditions. [6]

This article focuses on those two vulnerabilities. On 23 October 2026, the PHP project also published a separate informational advisory for CVE-2026-115560, a potential remote-code-execution issue requiring an unusual combination of configuration and application code. [8] [9] The project recommended disabling session upload progress pending a regular bug-fix release; the initial PHP2Shell updates should not be assumed to resolve this separate issue. [8] [9]

The disclosure quickly developed into an international coordination exercise. Authorities and national cyber-response bodies in the United Kingdom, European Union, United States and Japan issued urgent guidance asking organisations to identify affected systems, prioritise internet-facing services, apply security updates and investigate possible compromise. [7] [9] [10] [11] The response shows how a weakness in a common software component can create governance questions across multiple jurisdictions.

Response from UK, EU, US and Japan

United Kingdom

The UK National Cyber Security Centre (NCSC) encouraged organisations to take immediate action. [10] Its guidance emphasised identifying PHP installations,

prioritising internet-facing services and checking commercial products and appliances that may contain PHP as an embedded component. [10] Where patching or temporary mitigation was not possible, organisations were advised to consider taking affected systems offline and to investigate for evidence of compromise. [10]

For security and compliance teams, the practical issue is evidence. Organisations may need to show which assets were assessed, which services were exposed, how remediation was prioritised, when suppliers were contacted and whether affected systems were checked for compromise.

European Union

The European Commission, ENISA, CERT-EU, Europol's European Cybercrime Centre and the CSIRTs Network issued a joint statement calling for immediate action. [11] The statement noted that commercial and open-source products may use PHP in the background, meaning that organisations could be exposed even when they were not aware of operating PHP directly. [11]

The statement also connected PHP2Shell with the EU Cyber Resilience Act (CRA). [11] Article 14 reporting obligations have applied since 11 September 2026, including the reporting by manufacturers of actively exploited vulnerabilities contained in products within scope; the main cybersecurity requirements apply from 11 December 2027. [11] [12] Using PHP does not, by itself, make an organisation subject to CRA manufacturer obligations. [12] The incident illustrates the dependency-management challenge facing manufacturers: identifying vulnerable components, monitoring exploitation, providing security updates and communicating appropriately with customers. The application of specific duties depends on the organisation's role, product and relevant provision, so organisations should obtain legal advice where necessary.

United States

The US Cybersecurity and Infrastructure Security Agency (CISA) called for immediate patching and added both vulnerabilities to its Known Exploited Vulnerabilities Catalogue on 26 October 2026. [7] [13] CISA advised organisations to inventory PHP installations, prioritise public-facing systems, monitor for suspicious PHP worker activity and take unsupported systems offline where they could not be secured. [7]

The Known Exploited Vulnerabilities Catalogue is particularly significant for US federal civilian agencies and also provides a risk-prioritisation signal for

organisations elsewhere. [13] Its use should complement, rather than replace, an organisation's own assessment of exposure, asset criticality and operational impact.

Japan

JPCERT Coordination Center (JPCERT/CC) published an alert on 22 October 2026 and updated it on 29 October 2026. [9] JPCERT/CC confirmed that PHP is widely used in Japan, urged users to apply fixed versions promptly and recommended investigating whether affected systems had been compromised. [9] It also advised administrators to check information from product and operating-system suppliers because PHP may be embedded in products or supplied through Linux distributions. [9]

The updated alert reported numerous published proof-of-concept claims and reports of exploitation attempts. [9] In its 29 October update, JPCERT/CC cited Dream's investigation, which reported traces suggesting successful compromise of a specific firewall product version and attempted lateral movement into internal networks. [9] These are third-party findings cited by JPCERT/CC, not a statement that JPCERT/CC independently confirmed those compromises. JPCERT/CC cautioned that exploitability depends on the PHP version, runtime environment and memory layout. [9] For Japanese organisations, the governance priority is therefore to combine rapid remediation with product-dependency checks and evidence-led compromise assessment.

Evidence of Exploitation and Reporting Limitations

CISA's addition of both vulnerabilities to its Known Exploited Vulnerabilities Catalogue indicates that evidence of exploitation met its inclusion criteria. [7] [13] Inclusion does not, by itself, establish the scale of compromise, successful exploitation of every affected configuration or compromise of any particular organisation. JPCERT/CC also reported numerous published proof-of-concept claims and reports of traffic attempting to exploit the vulnerabilities. [9] However, JPCERT/CC noted that successful code execution depends on factors including the PHP version, runtime environment and memory layout. [9] The balanced conclusion is that exploitation had been documented, while its success and impact remained environment-dependent.

Governance and Assurance Priorities

PHP2Shell tests more than patching capability: organisations must demonstrate how they identified affected dependencies, assessed exposure and verified risk

decisions across jurisdictions. IT leaders, CISOs and boards should focus on five priorities:

1. Maintain inventories covering internal systems, cloud services, appliances and supplier-managed products, identifying affected PHP versions, configurations and internet exposure.
2. Prioritise remediation using authoritative exploitation evidence, external exposure, business criticality and operational impact; verify fixes and document any temporary mitigation or isolation.
3. Record management and supplier notifications, and require critical suppliers to provide affected-product details, mitigations and update plans promptly.
4. Retain traceable assessments, decisions, accepted exceptions and their rationale, compensating controls, remediation records and retest results.
5. Check affected systems for prior compromise and coordinate emergency changes with incident response where exploitation may already have occurred.

Conclusion

PHP2Shell is a useful cross-border case study because the same technical weakness produced aligned but distinct national and regional responses across the United Kingdom, European Union, United States and Japan. The lasting lesson is that cyber assurance depends on visibility and evidence: organisations must be able to identify affected dependencies, act in proportion to exposure and demonstrate how risk decisions were made, implemented and verified.

Technology Insights



Kanari Hirano
Associate Cybersecurity Engineer, Cybersecurity Service

Understanding Qilin, and Protecting Data

Summary: Qilin is a hacker group that rents its ransomware to affiliates, steals data before locking it. They attack companies of all industries and sizes, targeting devices and environments such as Windows, Linux, ESXi, and VMware environments.

Key points:

- Qilin is one of the most active ransomware groups. Its affiliates often get in with stolen credentials or flaws in VPN and firewall devices, then use double extortion to pressure victims.
- Suggested defence is strong multi-factor authentication (MFA), fast patching, limited access, and tested offline backups, backed by round-the-clock detection.

High-level overview of Qilin

Qilin, formerly known as Agenda, is a ransomware-as-a-service (RaaS) group that formed in 2022. The first samples of Agenda's ransomware appeared in August 2022, and the group renamed itself Qilin the following month, after a creature in Chinese mythology.[15] [16] [21] [29] The FBI defines ransomware as 'a type of software that prevents you from accessing computer files, systems, or networks and demands you pay a ransom for their return.'[14] Qilin goes a step further with double extortion by stealing data before encryption, and threatening to publish the data if the ransom isn't paid. In Qilin's RaaS business model, a core development team supplies the tools and infrastructure while recruited affiliates break into victims and carries out the attacks.[15] [16] [17] [29]

Qilin's ransomware, written in Go and later Rust, targets servers using Windows, Linux and VMware ESXi. Within the few years Qilin has been spotted, they have become one of the most active ransomware operations in the world.[18] [21] [29]

Qilin by the Numbers

- **Pace:** Check Point recorded 338 Qilin victim postings in the first quarter of 2026 and 279 in the second, making Qilin the most prolific ransomware operation for four consecutive quarters. By July it accounted for about 14% of publicly reported victim postings Check Point tracks. Leak-site postings are claims, not a verified count of successful attacks.[21]
- **Reach:** According to Japan's National Police Agency says Qilin has targeted about 4,000 organizations worldwide.[22]
- **Entry:** Intrusions frequently begin with valid credentials that were leaked on criminal channels between roughly one week and three months before use.[18]
- **Dwell time:** In 2025 incident-response casework, the ransomware executed an average of 6.1 days after the intrusion was first detected.[18]
- **Recovery:** As of November 2026, there is no way to crack any of Qilin's ransomware encryption unless the key is directly provided from them.[18]

Engagements with Law Enforcement

Law enforcement has directly engaged with the Qilin group when a 28-year-old Russian national. German authorities suspected this member as the leading member of Qilin. They were arrested in Japan in May 2026 and transferred to Germany on October 2.[20] [21] Although German authorities stated that investigators had infiltrated Qilin's before the arrest, the group should still be treated as an active threat as there is no public indication that Qilin has been dismantled.[21]

Ransomware Characteristics

Qilin's ransomware is built to work on many types of systems and to be hard to stop or undo. The main points:

- **Works on many systems.** It is written in modern programming languages (Go, later Rust), so the group can quickly make versions for Windows, Linux and VMware ESXi servers.[19][29] Attacking a virtualization server can take down many servers at once.[35]

- **Customizable by affiliates.** Affiliates choose which files to skip and which programs to shut down. The ransomware will not run without the right password, which makes it harder for researchers to study.[33] [34]
- **Strong encryption.** Files are locked with strong, modern encryption, so they cannot be recovered without the attacker's key. The newer "Qilin.B" version, released in October 2024, added stronger protection.[18] [21] [29] [33]
- **Disables defenses first.** Before encrypting, it turns off security and backup tools and deletes built-in Windows recovery copies. It can also spread to other computers on the network.[33] [34]
- **Leaves a ransom note and covers its tracks.** It drops a note with payment instructions, then erases logs and deletes itself to make investigation harder.[33] [34]

What Makes Qilin Stand Out from Other Hacker Groups?

Within a few years, Qilin became one of the most prolific ransomware operations in the world. It claimed 1,358 victims between April 2025 and March 2026, a 443% increase over the previous 12 months and roughly one in every five to six publicly disclosed ransomware victims worldwide.[18] Four things set it apart:

A franchise-style affiliate model.

Qilin's core operators supply the ransomware, leak site and negotiation infrastructure, while affiliates recruited on cybercrime forums carry out the intrusions. German investigators say Qilin works with several hundred affiliates.[16] [21] Affiliates reportedly keep about 80% of ransom payments under $3 million and 85% of larger ones, so Qilin keeps roughly 15–20%.[15] [16] [29]

Cross-platform tools and double extortion.

Its ransomware targets Windows, Linux and VMware ESXi servers. Affiliates steal data before encrypting it, then threaten to publish it if the victim does not pay.[15] [17] In the Nissan Creative Box attack, Qilin claimed about 4 TB of stolen data, including 3D vehicle models and other design files, and Nissan confirmed that some design data had leaked.[28]

Opportunistic targeting.

Qilin has no favorite industry. Professional services lead in KELA's data and manufacturing leads in other reports, and healthcare ranks high in both.[18] [19] [29] Victims tend to be large, high-value organizations that are potentially less secure.

Staying power

Many well-known ransomware brands did not last. Law enforcement disrupted LockBit in February 2024, BlackCat (ALPHV) collapsed in March 2024 after an apparent $22 million payment by Change Healthcare, and RansomHub went dark on April 1, 2025.[30] [31] [32] Qilin has outlived them: RansomHub's affiliates fled to Qilin, and the group has kept operating through 2026, with no public indication that it has been dismantled even after the arrest of a suspected leading member.[21] [32] The difference is resilience. When a rival group is taken down or disappears, its affiliates need a new platform, and Qilin's franchise-style model gives them one.

Qilin's Operation

Initial access, persistence and escalation:

Because affiliates bring their own access methods, Qilin intrusions do not follow a single fixed chain. Documented methods include phishing emails, software and operating-system vulnerabilities, hacked RDP services, and stolen credentials from underground forums.[18] [21] [29] Once inside, Qilin sets up its malware manually so that it persists and resists removal, and it escalates privileges through weak system configurations or legitimate admin tools.[29]

Edge devices:

Internet-facing devices became a major way in during 2026. In June, Check Point researchers assessed with medium confidence that an actor exploiting a Check Point VPN vulnerability (CVE-2026-50751) used Qilin ransomware, and CISA added the flaw to its Known Exploited Vulnerabilities catalog. In July, Arctic Wolf linked Qilin attacks to exploitation of CVE-2026-0257, a PAN-OS VPN authentication bypass.[21]

Evasion and lateral movement:

Qilin avoids detection by obfuscating code, using anti-analysis techniques, removing indicators, applying registry commands, and restarting systems in Safe Mode. To spread across the network, it uses network enumeration, credential theft and legitimate software tools.[29]

Data exfiltration and encryption:

Affiliates typically steal data before deploying ransomware, then use both encryption and the threat of publication as leverage. They exfiltrate data with free file transfer tools and encrypts the customer's data with techniques that

combine symmetric and asymmetric encryption. A custom ransom note is then delivered to the victim.[21] [29]

Negotiation, leak site and cleanup:

The ransom note directs victims to a dark web portal or encrypted chat to begin negotiating. Qilin controls the conversation and may offer to decrypt files as proof. Victims that do not pay can be listed on the leak site, sometimes with a countdown before files are released. If a ransom is paid, Qilin deletes system logs and other evidence of the attack.[21] [29]

Dark web presence:

Qilin's dark web infrastructure is private and supports both extortion and recruitment. It uses Tor to leak data and cybercrime forums to attract affiliates.[29]

Comparison with other groups:

Qilin's tactics closely mirror those of other ransomware groups. Its methods are not unique, but they show moderate sophistication within the ransomware, including code customization and multiple-platform capabilities.[29]

Analysing Attack Patterns: 2 Examples

Asahi Beer

On September 29, 2025, Asahi Group Holdings reported a system failure caused by a cyberattack that suspended orders, shipments and customer service across its Japanese operations.[26] Beer production restarted at its six domestic plants on October 2.[25] Qilin claimed the attack on October 7, saying it had stolen about 27 GB of data.[25] [26] Asahi later confirmed that the personal information of about 1.5 million customers, employees and contacts was compromised, and its investigation found that the attackers got in with stolen passwords.[27] **The lesson:** a single stolen password can halt production at a major manufacturer.

October 2026: Qilin's attacks on 53 Companies in Japan

On October 8, 2026, Japan's National Police Agency stated that 53 companies in Japan have been targeted by Qilin, with the group's activity in Japan confirmed since April 2023. The 53 Japanese victims span manufacturing, services, construction, hospitals and schools, including car-sharing service "Times Car", convenience store chain "Lawson", karaoke store chain "Daiichokosho".[22] These attacks served as an example on the dangers of outdated cybersecurity practices are against modern threats, such as AI. This incident indicated that AI

accelerated cyberattacks reduced the amount of time and money required to justify an attack, making any organization a possible target.

Overall Suggestions

The two cases hit different targets in different ways: a production line and design secrets, and exploiting old practices. They share the same weak points: stolen credentials, flat networks, and data that was easy to steal and use for extortion. We recommend these priorities:

1. **Lock down credentials and shrink the exposed surface.**

Qilin intrusions often begin with valid credentials, and VPN and firewall appliances are a common way in, as the Check Point VPN and PAN-OS flaws show. Require phishing-resistant MFA on all remote access, VPN and service accounts, monitor for leaked employee credentials, patch internet-facing systems quickly and retire unused remote access.[18] [21] [24] [27]

2. **Limit the blast radius with zero trust and data protection.**

One stolen account should not reach every data center or lab system, so use least-privilege access and network segmentation. Because of double extortion, restoring from backup does not undo a leak, so find where sensitive data lives, encrypt it, and use data loss prevention to stop it leaving.[15]

3. **Detect, respond and prepare to recover.**

Ransomware ran an average of 6.1 days after the intrusion was first detected, which leaves time to catch it. Managed detection and response (MXDR) services like Exaforce, along with human analysts can use that window around the clock.[18] Keep offline backups that are disconnected from the systems they protect, test them, and write manual fallback procedures that include key suppliers.[14] [18] [23] [28]

Suggestions

Protection, Prevention and Takeaways

1

The CenterPoint Energy and Burger King Japan breaches highlight the risks associated with internet-facing applications containing large volumes of personal information. Organisations should continuously identify and monitor their external attack surface, regularly scan and penetration-test public-facing systems, and prioritise remediation of exploitable vulnerabilities.

2

Effective segmentation, monitoring and incident response can significantly limit the impact of a compromise. Customer-facing applications, corporate IT and critical operational environments should be appropriately separated, while centralised logging, SIEM and endpoint monitoring should be used to identify suspicious behaviour. Regularly tested incident-response procedures should cover data breaches, credential compromise and software supply-chain incidents, enabling affected credentials, systems and applications to be rapidly identified, isolated and recovered.

3

How resilient are your staff to cyber attacks? When was the last time your organisation has phishing training, not just for email but for text and voice? Running annual campaigns for email phishing is no longer enough and was arguably never enough to prepare staff for the threats posed by malicious actors. Businesses need to do more to make sure that their staff can identify advances from threat actors. Frequent training should incorporate not just email simulations, but all manner of tactics used by threat actors including deepfakes.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This month it is 2 related vulnerabilities affecting a large majority of web servers on the internet. PHP2Shell is the popular name given to these vulnerabilities affecting PHP.

CVE-2026-109618 & CVE-2026-109619

[EUVD-2026-107260 & EUVD-2026-107265] [36] [37]

	CVE-2026-109618 | EUVD-2026-107260	CVE-2026-109619 | EUVD-2026-107265
Vendor	PHP Group	
Product	PHP	
Publish Date	October 21, 2026	
Platform	PHP web-serving installations, including Apache mod_php, PHP-FPM, CGI, FrankenPHP, and LiteSpeed	
CVSS (v3.1)	9.8	8.1

Description

CVE-2026-109618: An out-of-memory handling flaw can cause PHP to treat partially initialised request data as valid during cleanup. It may allow remote code execution and memory disclosure.

CVE-2026-109619: A use-after-free flaw leaves stale internal state that a later request may use, potentially enabling remote code execution.

What does this mean for you?

If a website or app runs an unpatched PHP server, an attacker could potentially take control of that server and access or alter its data.

What should you do about it?

Update PHP immediately to 8.2.35, 8.3.36, 8.4.27, or 8.5.12the fixed version for your branch. If PHP comes from your operating-system vendor or hosting provider, install its patched package.

References

1. ProtectMyData (2026) ‘CenterPoint Energy Data Breach: What Texans Should Know’, ProtectMyData, 19 October. Available at: https://protectmydata.com/blog/news/centerpoint-energy-data-breach-2026 (Accessed: 29 October 2026).
2. Gatlan, S. (2026) ‘Burger King Japan data breach exposes 11 million customer records’, BleepingComputer, 16 October. Available at: https://www.bleepingcomputer.com/news/security/burger-king-japan-data-breach-exposes-11-million-customer-records/ (Accessed: 5 November 2026).
3. Arctic Wolf (2026) Beyond the inbox: how threat actors abuse Microsoft Teams external chat for initial access. Available at: https://arcticwolf.com/resources/blog/threat-actors-abuse-microsoft-teams-external-chat-for-initial-access/ (Accessed: 11 Oct 2026).
4. Infosecurity Magazine (2026) Attackers exploit Teams external chat to breach organizations in under an hour. Available at: https://www.infosecurity-magazine.com/news/exploit-teams-chat-breach/ (Accessed: 18 Oct 2026).
5. Techzine (2026) Attackers are exploiting Teams chat as a fake IT help desk. Available at: https://www.techzine.eu/news/security/145269/attackers-are-exploiting-teams-chat-as-a-fake-it-help-desk/ (Accessed: 16 Oct 2026).
6. The PHP Group (2026) Security advisory: Critical remote code execution vulnerabilities, update now. 21 October. Available at: https://www.php.net/archive/2026.php (Accessed: 31 October 2026).
7. Cybersecurity and Infrastructure Security Agency (CISA) (2026) Critical Vulnerabilities in PHP Require Immediate Patching. 21 October. Updated 26 October 2026. Available at: https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching (Accessed: 31 October 2026).
8. The PHP Group (2026) Informational advisory: Session upload progress. 23 October. Available at: https://www.php.net/archive/2026.php (Accessed: 31 October 2026).
9. JPCERT Coordination Center (JPCERT/CC) (2026) PHP における複数の脆弱性（CVE-2026-109618、CVE-2026-109619）に関する注意喚起. JPCERT-AT-2026-0033. 22 October. Updated 29 October 2026. Available at: https://www.jpcert.or.jp/at/2026/at260033.html (Accessed: 31 October 2026).

10. National Cyber Security Centre (NCSC) (2026) Critical security issue affecting PHP. 21 October. Available at: https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php (Accessed: 31 October 2026).
11. European Commission (2026) Joint statement on critical PHP vulnerabilities. 21 October. Available at: https://digital-strategy.ec.europa.eu/en/news/joint-statement-critical-php-vulnerabilities (Accessed: 31 October 2026).
12. European Parliament and Council of the European Union (2024) Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 2, 3, 14 and 71. 23 October. Official Journal, 20 November 2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (Accessed: 31 October 2026).
13. Cybersecurity and Infrastructure Security Agency (CISA) (2026) Known Exploited Vulnerabilities Catalog. Available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog (Accessed: 31 October 2026).
14. FBI (n.d.) 'Ransomware', FBI. Available at: https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/ransomware (Accessed: 4 November 2026).
15. Check Point Software (n.d.) 'Qilin Ransomware (Agenda): A Deep Dive', Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/qilin-ransomware/ (Accessed: 4 November 2026).
16. SANS Institute (2025) 'The Evolution of Qilin RaaS', SANS Institute, 3 October. Available at: https://www.sans.org/blog/evolution-qilin-raas (Accessed: 4 November 2026).
17. Acronis Threat Research Unit (2026) 'Inside Qilin ransomware: ESXi attacks, affiliate networks and double extortion', Acronis Threat Research Unit, 28 October. Available at: https://www.acronis.com/en/tru/posts/inside-qilin-ransomware-esxi-attacks-affiliate-networks-and-double-extortion/ (Accessed: 4 November 2026).
18. Adaptive Security (2026) 'Qilin Ransomware: How It Attacks, Who It Has Hit, and How to Defend Against It', Adaptive Security, 6 September. Available at: https://www.adaptivesecurity.com/blog/qilin-ransomware (Accessed: 4 November 2026).
19. ThreatLocker (2025) 'Qilin Ransomware: Technical analysis, from initial access to beaconing', ThreatLocker, 29 October. Available at: https://www.threatlocker.com/blog/qilin-raas-group-technical-analysis-from-initial-access-to-beaconing (Accessed: 4 November 2026).
20. The Asahi Shimbun (2026) 'Japan collars fugitive suspect of ransomware syndicate Qilin', The Asahi Shimbun, 6 October. Available at: https://www.asahi.com/ajw/articles/16943165 (Accessed: 4 November 2026).

21. BreachNews (2026) ‘Qilin Ransomware: Attacks, Victims and Latest Activity’, BreachNews, updated 28 October. Available at: https://breachnews.com/threat-actors/qilin/ (Accessed: 4 November 2026).
22. The Straits Times (n.d.) ‘53 companies in Japan hit by Qilin ransomware group: police agency’, The Straits Times. Available at: https://www.straitstimes.com/asia/east-asia/53-companies-in-japan-hit-by-qilin-ransomware-group (Accessed: 4 November 2026).
23. NHS England (2025) ‘Synnovis cyber incident’, NHS England, 10 November. Available at: https://www.england.nhs.uk/synnovis-cyber-incident/ (Accessed: 4 November 2026).
24. Safeguard (2026) ‘Synnovis NHS Qilin Ransomware: Pathology Supply Chain Lessons’, Safeguard, 9 January. Available at: https://safeguard.sh/resources/blog/synnovis-nhs-qilin-ransomware-pathology-supply-chain (Accessed: 4 November 2026).
25. The Asahi Shimbun / Reuters (2025) ‘Japan’s Asahi hack that halted beer production claimed by Qilin ransomware group’, The Asahi Shimbun / Reuters, 8 October. Available at: https://www.asahi.com/ajw/articles/16077955 (Accessed: 4 November 2026).
26. Comparitech (2025) ‘Ransomware gang Qilin says it hacked Asahi Group, stole data’, Comparitech, 7 October. Available at: https://www.comparitech.com/news/ransomware-gang-qilin-says-it-hacked-asahi-group-stole-data/ (Accessed: 4 November 2026).
27. Rescana (2025) ‘Asahi Group Holdings Ransomware Attack: Qilin Breach Disrupts Japanese Operations and Exposes 1.5 Million Records’, Rescana, 30 November. Available at: https://www.rescana.com/post/asahi-group-holdings-ransomware-attack-qilin-breach-disrupts-japanese-operations-and-exposes-1-5-mi (Accessed: 4 November 2026).
28. BleepingComputer (2025) ‘Nissan confirms design studio data breach claimed by Qilin ransomware’, BleepingComputer, 26 August. Available at: https://www.bleepingcomputer.com/news/security/nissan-confirms-design-studio-data-breach-claimed-by-qilin-ransomware/ (Accessed: 4 November 2026).
29. KELA Cyber (2025) ‘Who Is the Qilin Ransomware Group and How Do They Operate?’, KELA Cyber, 25 August. Available at: https://www.kelacyber.com/blog/who-is-the-qilin-ransomware-group-and-how-do-they-operate/ (Accessed: 4 November 2026).
30. Europol (2024) ‘Law enforcement disrupt world’s biggest ransomware operation’, Europol, 20 February. Available at:

https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation (Accessed: 4 November 2026).
31. Krebs on Security (2024) 'BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare', Krebs on Security, 5 March. Available at: https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/ (Accessed: 4 November 2026).
32. The Hacker News (2025) 'RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control', The Hacker News, 30 April. Available at: https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html (Accessed: 4 November 2026).
33. Halcyon RISE Team (2024) 'New Qilin.B Ransomware Variant Boasts Enhanced Encryption and Defense Evasion', Halcyon RISE Team, 24 October. Available at: https://www.halcyon.ai/blog/new-qilin-b-ransomware-variant-boasts-enhanced-encryption-and-defense-evasion (Accessed: 4 November 2026).
34. Malware Cake Factory (2026) 'Qilin Ransomware (Rust Variant) Analysis', Malware Cake Factory, 7 March. Available at: https://malwarecakefactory.github.io/malware-analysis/qilin-ransomware-rust-analysis/ (Accessed: 4 November 2026).
35. shadowshell.io (2024) 'Reversing the Qilin ESXi ransomware', shadowshell.io, 25 September. Available at: https://shadowshell.io/qilin-ransomware (Accessed: 4 November 2026).
36. ENISA (2026) 'EUVD-2026-107260', European Union Vulnerability Database, 21 October. Available at: https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-107260 (Accessed: 4 November 2026).
37. VulDB (2026) 'CVE-2026-109619 PHP PHP2Shell race condition (EUVD-2026-107265 / Nessus ID 370149)', 21 October. Available at: https://vuldb.com/vuln/424815 (Accessed: 4 November 2026).

Let’s Secure the Future — Together

KDDI America

KDDI America is the North American headquarters of KDDI Corporation, a Fortune Global 500 company, delivering cloud, networking, cybersecurity, and managed IT services. Through innovative ICT solutions, KDDI America helps organisations connect, transform, and grow in an increasingly digital world.

KDDI Europe

KDDI Europe is the European headquarters of KDDI Corporation, a Fortune Global 500 company, delivering trusted ICT and cybersecurity solutions backed by Japanese quality and reliability. With over 70 years of global expertise, we help organisations build secure, scalable infrastructure and strengthen their cyber resilience.

Whether you’re looking to strengthen your cybersecurity posture or scale your global operations, we are your partner, your enabler, your platformer.

Security of Tomorrow, Today.

Contact Information

KDDI Europe	Website	LinkedIn	Enquiry
KDDI America	Website	LinkedIn	Enquiry