It's Probably Nothing
by Sierra Echo Charlie

EDITION 15 / 28 OCTOBER 2026

Real booking details make a better payment scam

Plus PHP2Shell's KEV escalation, a Consul namespace bypass and casino crypto flows.

4 stories / Listen online - 2:51

THE TAKEAWAY

The uncomfortable bit of the holiday-park story is how little a convincing payment scam needs: the right name, the right dates and a plausible request.

01 / THE BRIEF

Genuine bookings, fraudulent payment requests

ABC reports Australian holiday-park operators are warning guests about payment scams following an incident involving RMS Cloud's booking platform. RMS says it's investigating WhatsApp, SMS and email messages that reference genuine booking information and request payment details. A Victorian park manager told ABC the names and dates of stay were correct.

RMS says no payment-card information has been exposed from RMS. That's a narrow reassurance: booking details can supply the credibility while the message asks for the card. The intrusion route, initial-access date and affected population remain unresolved.

SOURCES

Major holiday park operators warn guests about fraudulent emails, messages seeking credit card details - Reporting / context

02 / THE BRIEF

PHP2Shell moves from patching to forensic triage

CISA has added both PHP2Shell vulnerabilities, CVE-2026-109618 and CVE-2026-109619, to its known-exploited catalogue, dated 26 October. Covered US federal agencies must carry out forensic triage and remediate by 29 October.

That's a meaningful escalation from the previously reported attack attempts, not evidence of widespread successful compromise. Patching and investigating are now explicitly separate jobs.

PHP still puts all installations serving web requests in the at-risk population, with the highest demonstrated risk in mod_php, where exploitation can precede application code. The fixes remain PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35. PHP says configuration mitigations aren't a complete solution.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

Critical Vulnerabilities in PHP Require Immediate Patching - Primary source

PHP: News Archive - 2026 - Primary source

Rapid Response: php2shell, Leaked Critical PHP Vulnerabilities - Primary source

PHP Releases Emergency PHP2Shell RCE Fixes as Attack Attempts Prompt Website Shutdowns - Reporting / context

03 / THE BRIEF

Consul component privileges from the wrong namespace

If you run consul-k8s with global.acls.manageSystemACLs=true, CVE-2026-110720 is worth checking. HashiCorp says an attacker who can create a ServiceAccount and obtain its token in another namespace, and reach the Consul API, may authenticate as a Consul component and obtain its associated privileges.

The failure is insufficient namespace restrictions in component binding rules: an awkward boundary failure for shared clusters. Deployments with system ACL management disabled aren't vulnerable. HashiCorp supplies fixes in consul-k8s 1.8.18 and 2.1.0.

SOURCES

HCSEC-2026-50 - Consul-k8s vulnerable to a cross-namespace authorization bypass in component ACL binding rules - Primary source

04 / THE BRIEF

Sanctions haven't stopped the casino crypto flows

TRM Labs attributes approximately US$1.07 billion in crypto receipts to 34 physical Sihanoukville casinos between 1 January and 7 September 2026. More pointedly, it reports approximately US$322 million received after the relevant designation dates by entities it attributes to Xihu, Huan Hai and a Jin Bei Group-associated casino.

These are TRM's attributions, not independently verified totals or proof that every receipt was criminal. TRM also cautions that wallet rotation may make declining attributed inflows overstate the actual reduction in activity. Losing sight of the money isn't the same as stopping it.

SOURCES

Crypto Continues to Flow Through Sihanoukville Casinos Despite Cambodia's Crackdown - Primary source

Sihanoukville Casinos Receive $1.07 Billion in Crypto Despite Sanctions and Crackdowns - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.