

Three critical cyber weaknesses. One business priority: Act now.

Three flaws affecting different parts of the technology your business relies on: websites, digital certificates and Linux-based cloud infrastructure.

Each can disrupt operations, expose data and undermine trust.



Why this matters now

Amazon detected a **PHP2Shell** exploitation attempt on 17 October, before public disclosure and patch availability on 21 October 2026.

CERT-In has warned about compromised **eMudhra** certificate-authority keys.

Google removed the affected **emSign** root from the Chrome Root Store, with the change expected to reach dependent devices from 27 October 2026.

Organisations must urgently identify vulnerable PHP systems and any certificates that rely on the affected trust chain.

What the issues are

PHP2Shell Websites at risk

What it is

- **PHP** technology is widely used to run websites and web applications
- The issue allows an attacker to **gain access** to vulnerable systems without logging in
- It is a **PHP platform weakness**, not a flaw in the application code

Business impact

- A website could be **altered** or **taken over**
- Data can be exposed. Passwords and access keys can be stolen

Remediation

- Identify internet-facing system running **PHP**, upgrade and retest
- The advisory lists **PHP 8.5.12**, **8.4.27**, **8.3.36** or **8.2.35**

eMudhra certificates Digital trust at risk

What it is

- eMudhra certificates help websites and software prove **trustworthiness**
- eMudhra certificate-signing keys were reportedly **weak** enough to recover from public certificates

Business impact

- Affected websites may show browser security warnings after 27 October 2026
- Two keys could sign software Windows might trust, thus allowing **malicious software** to appear legitimate

Remediation

- Identify certificates that rely on the affected **eMudhra** trust chain and replace
- Never bypass certificate warnings

PwnEscape Cloud infrastructure at risk

What it is

- **PwnEscape** affects Linux systems used to host virtual machines
- The flaw may let isolated virtual machines access memory belonging to its **host server**

Business impact

- Sensitive host memory could be exposed or workloads on the host could crash
- Cloud providers, hosting companies and organisations running Linux hosts may be affected

Remediation

- The party responsible for the Linux host must patch and restart it, then verify the fix
- Updating only the guest virtual machine does not fix the host

What this means for your organisation

These **vulnerabilities** could disrupt **websites** and **cloud services**, expose **sensitive data**, **credentials**, and weaken trust in digital services.

The consequences could include **recovery costs**, **lost revenue**, **customer attrition** and **regulatory scrutiny**.

How #GTBharat can support

Our team of experts can assess your 'crown jewel', identify PHP2 shell weaknesses, e-mudra certificate failures and Linux server issues, and provide a prescriptive report and help secure your business.

If you are a function owner, such as CDO, CIO, CISO or similar, please read on.

CISO response checklist: Identify, remediate, verify

Operational view for application, certificate and infrastructure teams

Issue	Exposure to confirm	Remediation	Validation
PHP2Shell Critical	<ul style="list-style-type: none">Inventory internet-facing PHP systems, including legacy and vendor-hosted assetsConfirm installed versions and exposure	<ul style="list-style-type: none">Upgrade to a fixed version listed in the advisory: PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35Coordinate change and rollback plans	<ul style="list-style-type: none">Record before/after versionsRun targeted security testing and confirm vulnerable condition is absentMonitor for suspicious activity
eMudhra certificates Critical	<ul style="list-style-type: none">Locate affected certificates across websites, APIs, apps, appliances, runtimes and containersMap owners and dependencies	<ul style="list-style-type: none">Replace affected certificates before 27 OctoberDo not bypass validation warningsCoordinate with service owners and vendors	<ul style="list-style-type: none">Keep replacement logsValidate certificate chains and application/API integrationsConfirm clients no longer rely on affected certificates
PwnEscape Critical	<ul style="list-style-type: none">Identify Linux host /hypervisor and cloud/hosting environmentsEstablish who owns patching for each host	<ul style="list-style-type: none">Patch and restart affected Linux host servers. A guest VM patch alone is insufficientCoordinate with providers and service owners	<ul style="list-style-type: none">Collect patch/reboot evidence and provider attestationsConfirm workload stabilityReview host-level telemetry where available

Cross-cutting controls from the advisory

Attack surface Maintain a live inventory of internet-facing systems, including older and vendor-hosted assets.	Patch SLA The advisory cites 12 hours for known-exploited internet-facing flaws and one day for other critical flaws. Confirm policy and applicability.	Vendor accountability Require cloud, hosting and software providers to confirm fixes with evidence.
Continuous testing Retest every fix. Include APIs and externally exposed services in security testing.	Detection and reporting Monitor critical systems and follow applicable CERT-In reporting requirements; advisory cites six hours for covered incidents.	Certificate hygiene Track issuer, owner, usage and dependencies; maintain a tested replacement process.

Suggested 24-hour response sequence

0-2 hours

- Assign response lead
- Notify application, infrastructure, certificate and vendor owners
- Begin exposure discovery

2-12 hours

- Prioritise confirmed exposure
- Patch PHP where applicable
- Initiate certificate replacement
- Obtain host-provider action plans

12-24 hours

- Complete or track critical fixes
- Validate services, retest and review telemetry
- Escalate unresolved exposure with an approved risk decision

Connect with our experts

 <p>Ravi Prakash Partner, Cyber Advisory Grant Thornton Bharat E: ravi.prakash@in.gt.com</p>	 <p>Apoorba Patranabish Partner, Cyber Advisory Grant Thornton Bharat E: apoorba.patranabish@in.gt.com</p>
 <p>Kush Wadhwa Partner, Cyber Advisory Grant Thornton Bharat E: kush.wadhwa@in.gt.com</p>	 <p>Manish Anand Associate Partner, Cyber Advisory Grant Thornton Bharat E: manish.anand@in.gt.com</p>