Macksofy TECHNOLOGIES

CERT-In EMPANELLED
INFORMATION SECURITY AUDITOR
MUMBAI · DUBAI · TORONTO

RESEARCH NOTE / REGULATORY / INDIA

CERT-In’s 12-Hour Patch Mandate

India’s AI-paced patching standard — the tiered schedule, the exploit-window collapse that justifies it, and what Indian organisations should actually do.

PREPARED BY
Macksofy Audit Team · Compliance & Regulatory Practice

PUBLISHED
30 May 2026 · Mumbai

12:00:00
THE NEW REMEDIATION WINDOW

01 The signal

On **25 May 2026**, CERT-In published its AI Threat Landscape guidance and, with it, an indicative 12-hour expectation for containing or remediating known exploited vulnerabilities (KEVs) on internet-facing and high-value “crown-jewel” systems. The number is neither arbitrary nor aspirational — it is calibrated to how fast AI-assisted attackers now weaponise a disclosed flaw.

The headline is the timeline. The more consequential shift is the benchmark CERT-In chose: India’s national cybersecurity authority is now pacing remediation expectations against AI-driven threat timelines rather than legacy IT change-management windows. Read it as a leading indicator of where patch-compliance standards are heading everywhere — not an India-only curiosity.

02 What was actually published

The guidance establishes a **tiered** remediation schedule keyed to the intersection of vulnerability severity and system-exposure profile — not a single deadline applied to everything. This is risk-based prioritisation, and it materially reduces the operational burden relative to a flat 12-hour rule. The 12-hour window applies narrowly: to vulnerabilities already exploited in the wild and catalogued in threat-intelligence feeds, affecting systems directly exposed to the internet or classified as high-value internal assets.

WINDOW	VULNERABILITY & EXPOSURE PROFILE	WHAT QUALIFIES
12 hrs	**KEV on internet-exposed / high-value system**	Already exploited in the wild; internet-facing or crown-jewel asset.
24 hrs	**Critical, not yet exploited, externally exposed**	Critical severity with external exposure but no confirmed exploitation.
3 days	**Critical on internal high-value system**	Critical severity, high-value, not directly internet-facing.
5 days	**High-severity, below critical threshold**	High-severity flaws outside the critical band.

CERT-In TIERED REMEDIATION SCHEDULE · INDICATIVE · 25 MAY 2026

> INDICATIVE — NOT STATUTORY, YET
>
> *CERT-In framed these timelines as indicative expectations, not legally binding obligations. The operational signal is nonetheless unambiguous. The 6-hour incident-reporting direction began the same way before it hardened — treat the 12-hour figure as the direction of supervisory expectation, not a clause to ignore until enforced.*

03 Why 12 hours — the exploit window has collapsed

The window reads less like an aspirational benchmark and more like a recognition of what attackers armed with AI tooling already achieve. The standard was calibrated to attacker capability, not defender comfort. The empirical basis is a measurable collapse in the time between CVE publication and active exploitation.

~56d→10h

Average CVE-to-exploit window, 2024 vs mid-2026.

SYNACK / HELP NET SECURITY 2026

28.3%

of CVEs now exploited within 24 hours of disclosure — a negative time-to-exploit trend.

MANDIANT M-TRENDS 2026

51% @ $2.77

of 2024–25 CVEs auto-reproduced as working exploits, per-CVE cost.

CVE-GENIE RESEARCH, 2026

AI frameworks that generate working exploits from a CVE description in ten to fifteen minutes, at trivial cost, have rewritten the economics of weaponisation. Exploitation increasingly *precedes* vendor-patch availability. Any organisation maintaining 30-day — or even 7-day — windows for internet-exposed systems is running a risk posture formulated before the current AI capability environment existed.

04 It builds on the 6-hour reporting rule

This is not CERT-In's first timeline to challenge legacy operations rhythms. Since 2022, Direction 20(3)/2022 has required organisations to report cybersecurity incidents within six hours of awareness — forcing Indian enterprises to restructure detection, escalation and internal communications. The patch guidance applies comparable urgency to the *remediation* side of the lifecycle. Together they point to one coherent posture: as AI compresses every phase of attack execution, defensive timelines must compress in parallel.

05 Where no patch exists — the compensating-control path

CERT-In explicitly accommodates the reality that the window cannot always be met through vendor-patch availability alone. The crucial nuance: the 12-hour deadline applies to the obligation to act, not exclusively to the obligation to patch. A documented containment measure implemented within 12 hours satisfies the intent of the standard.

- Network isolation
- Access restriction · auth-only
- WAF virtual patch at the edge
- Segmentation · JIT · protocol limits

For most Indian enterprises — and essentially all MSMEs — a tested compensating-control playbook is the realistic compliance pathway, and the work to invest in first. The obligation is to neutralise exposure, not merely to apply a fix.

06 India in the global patching-governance landscape

To our knowledge, India is the first major national authority to publish a tiered patch timeline explicitly calibrated to AI exploitation speed. The closest US analogue in design philosophy — CISA's Known Exploited Vulnerabilities catalog — currently averages roughly two weeks, with a three-day federal KEV standard reportedly under consideration but not finalised.

CERT-IN (INDIA) · MAY 2026

- 12 hours for KEVs on internet-facing / crown-jewel systems
- Tiered by severity × exposure (12h / 24h / 3d / 5d)
- Explicitly calibrated to AI exploitation speed
- Compensating controls accepted as interim compliance

CISA KEV (US) · 2026

- ~14-day average remediation deadlines
- Moving toward a 14-day default window
- Three-day KEV standard reportedly under consideration
- Same AI threat data informing the debate

The gap reflects different regulatory response timelines — not different threats. The same AI tooling targeting Indian infrastructure targets infrastructure globally. For multinationals, this argues for one unified prioritisation programme applying the most stringent applicable standard to all internet-facing assets by default.

07 The operational reality — the MSME gap

An honest assessment: most enterprises, and essentially all SMEs, cannot achieve consistent 12-hour deployment for internet-facing systems without real investment in automation, continuous asset monitoring and pre-tested pipelines. India's large MSME segment faces the steepest climb. That does not make the guidance irrelevant — it makes the compensating-control provisions essential.

08 What to do — next 30 / 60 / 90 days

01. Audit the internet-facing asset inventory and map it to CERT-In advisories and the CISA KEV catalog.
02. Integrate a near-real-time KEV threat-intelligence feed with automated alerting tied to that inventory.
03. Build and test a compensating-control playbook executable inside 12 hours when no patch exists.
04. Stand up low-friction emergency patch automation for the internet-facing tier, outside the full CAB process.
05. Run a tabletop: a CVE lands at 09:00 with confirmed exploitation — can the exposed tier be contained by 21:00?

How Macksofy helps

As a CERT-In empanelled auditor, Macksofy delivers the readiness this guidance demands: continuous VAPT against internet-facing assets, KEV-aligned threat-intelligence integration, compensating-control playbook design, and the emergency-remediation runbooks that make a 12-hour window operationally feasible — from a focused exposure-and-readiness assessment to a fully managed detect–correlate–contain programme.

FIXED-PRICE PROPOSAL	SPEAK TO A CONSULTANT	EMAIL
within 48 hours	**+91 99308 24239**	**services@macksofy.com**

09 Sources & attribution

PRIMARY GUIDANCE

— CERT-In, *AI Threat Landscape guidance*, 25 May 2026 (indicative tiered remediation schedule).

— CERT-In, Direction 20(3)/2022 (six-hour incident-reporting requirement).

ANALYSIS & DATA REFERENCED

— Cloud Security Alliance, research note: *CERT-In's 12-Hour Patch Mandate — AI-Paced Compliance*, 26 May 2026.

— Mandiant, *M-Trends 2026* (24-hour exploitation figure).

— Synack / Help Net Security, 2026 (CVE-to-exploit window).

— CVE-Genie, "From CVE Entries to Verifiable Exploits," arXiv preprint, 2026.

— CISA, Known Exploited Vulnerabilities catalog & reported federal-standard deliberations, 2026.

MACKSOFY COMMENTARY

— Full article: macksofy.com/blog/cert-in-12-hour-patch-mandate-ai-exploitation-2026