INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-27 14:08 UTC

# CERT-In Issues 12-Hour Patching Mandate for Internet-Facing Vulnerabilities Amid AI-Accelerated Exploitation

GOVERNANCE | HIGH

| | |
|---|---|
| SCC Item ID | SCC-GOV-2026-0040 |
| Type | Governance |
| Severity | HIGH |
| Affected Products | All organizations with internet-exposed systems, particularly those operating in India or under CERT-In jurisdiction |
| Published | 2026-05-26 |
| Discovery Source | Gemini |

## Executive Summary

CERT-In, India's national cybersecurity authority, has mandated that organizations patch critical vulnerabilities in internet-facing systems within 12 hours of public disclosure. This directive reflects regulatory response to accelerated exploitation timelines. Traditional 30/60/90-day patch cycles are no longer acceptable for internet-exposed assets under this mandate, and the regulatory pressure reflects a global trend toward mandatory accelerated remediation timelines. Organizations with internet-facing infrastructure, particularly those operating in India or under CERT-In jurisdiction, face compliance exposure and elevated operational risk if existing patch processes are not restructured immediately.

## Technical Analysis

This item addresses a regulatory directive from CERT-In, not a specific vulnerability disclosure. No individual CVEs, CWEs, or active campaigns are cited. CERT-In's updated guidance targets internet-facing systems broadly, with policy rationale anchored in accelerated exploitation capabilities, specifically automated vulnerability scanning (MITRE T1595.002: Vulnerability Scanning), proof-of-concept generation, and exploitation of public-facing applications (MITRE T1190: Exploit Public-Facing Application). The 12-hour remediation window applies to critical vulnerabilities in internet-exposed services at the point of public disclosure, not just at vendor patch release. Practitioners should verify current directive language and scope against the official CERT-In publication at cert-in.org.in before implementing compliance changes. CISA's Internet Exposure Reduction Guidance (Tier 1 source) provides complementary methodology for reducing attack surface on internet-facing systems.

## Action Checklist

1. Step 1: Scope. Inventory all internet-facing systems immediately using CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory). Identify which assets are exposed to the public internet, classify them by criticality, and flag any running software with known unpatched critical vulnerabilities. This inventory is the prerequisite for every subsequent step.
2. Step 2: Process gap assessment. Compare your current vulnerability remediation SLAs against the 12-hour window for internet-facing critical vulnerabilities. Document which systems, teams, and approval workflows would block compliance with this timeline. Reference NIST SI-4 (System Monitoring) for continuous visibility requirements and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) for process baseline.
3. Step 3: Detection and monitoring. Deploy continuous monitoring on internet-facing assets to detect active scanning and exploitation attempts. Log authentication events, service access, and anomalous outbound connections per NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting). Enable alerting on T1595.002-relevant indicators: high-rate scan traffic, automated user-agent strings, and sequential port probing against exposed services.
4. Step 4: Remediation acceleration. Establish an emergency patch track for internet-facing critical vulnerabilities with pre-approved change authority, eliminating standard change advisory board delays for this asset class. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for automation targets. Where patching within 12 hours is operationally infeasible, document a compensating control, such as WAF rule deployment, temporary service isolation, or virtual patching, as an interim measure.
5. Step 5: Post-directive hardening. Treat this mandate as an opportunity to reduce internet exposure surface by decommissioning or segmenting services that do not require public accessibility per CISA Internet Exposure Reduction Guidance. Apply D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) to all remaining internet-facing administrative interfaces. Document control gaps identified during scope assessment and assign remediation owners with tracked deadlines per NIST AC-6 (Least Privilege) and CIS 6.3 (Require MFA for Externally-Exposed Applications).

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate immediately to senior leadership and legal/compliance counsel if network monitoring (Step 3) detects active exploitation attempts against any internet-facing asset with an unpatched critical CVE, if the organization cannot demonstrate a credible path to 12-hour patch compliance for any CERT-In-regulated asset class within 72 hours, or if evidence of pre-patch compromise is found during the forensic imaging step — all three conditions trigger mandatory CERT-In breach reporting obligations under the 2022 CERT-In Directions. |

| | |
|---|---|
| **Recovery Notes** | After completing the emergency patch and compensating control deployment for each affected internet-facing system, conduct a focused compromise assessment on every asset that was exposed with an unpatched critical vulnerability for any duration — specifically checking for web shells in web root directories, unauthorized scheduled tasks or cron jobs, new local admin accounts, and persistence mechanisms (Windows: 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'; Linux: '/etc/cron.d/', '/etc/rc.local', systemd unit files in '/etc/systemd/system/'). Monitor all patched systems for 30 days post-remediation with elevated logging verbosity, paying particular attention to outbound connections to uncommon geolocations and anomalous process execution chains from previously vulnerable services — AI-automated exploitation frameworks often implant staged payloads that activate post-patch if initial access was achieved before remediation. Retain all forensic artifacts and the complete remediation timeline documentation for a minimum of 180 days to support any CERT-In regulatory inquiry. |
| **Forensic Artifacts** | Web server access logs (Apache: /var/log/apache2/access.log; nginx: /var/log/nginx/access.log; IIS: C:\inetpub\logs\LogFiles\W3SVC*\) — specifically entries containing AI-scanner user-agent strings (nuclei, python-requests, masscan, zgrab, Nmap Scripting Engine) or sequential URI enumeration patterns consistent with automated vulnerability probing against the disclosed CVE's affected endpoint or parameter \| Pre-patch forensic system image (VMware snapshot, AWS AMI, or dd image) capturing the exact system state during the window between CVE public disclosure and patch application — this is the primary artifact for determining whether exploitation preceded remediation and is required to establish regulatory timeline for CERT-In reporting \| Network flow records or perimeter firewall logs covering the period from CVE public disclosure to patch completion — filter on inbound connections to the vulnerable service port(s) from external source IPs to identify whether the asset received exploitation-pattern traffic during the unpatched window, which is direct evidence for the CERT-In 12-hour compliance gap assessment \| Windows Security Event Log Event ID 4688 (Process Creation) or Linux auditd execve records filtered on child processes spawned by the internet-facing service account (IIS AppPool, www-data, apache, tomcat) — unexpected cmd.exe, powershell.exe, bash, or curl/wget child processes are primary indicators of successful exploitation via AI-automated exploit delivery during the unpatched window \| File system timeline artifacts from web root directories (/var/www/html, C:\inetpub\wwwroot, and application-specific deploy paths) — run 'find -newer -type f' to identify files created or modified after CVE disclosure but before patching, which may indicate web shell implantation by automated exploitation tooling operating in the gap window between disclosure and remediation |

### Per-Action IR Details

**Step 1: Scope — Inventory all internet-facing systems immediately using CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory). Identify which assets are exposed to the public internet, classify them by criticality, and flag any running software with known unpatched critical vulnerabilities. This inventory is the prerequisite for every subsequent step.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Establishing IR Capability and Asset Visibility

**Controls:** CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST CM-8 (System Component Inventory), NIST RA-5 (Vulnerability Monitoring and Scanning)

**Compensating:** Run 'nmap -sV --open -p 80,443,8080,8443,22,3389,21,25,53 -oX internet_facing_$(date +%F).xml' from an external vantage point to enumerate publicly reachable services. Cross-reference output against internal CMDB or spreadsheet inventory. For software version identification on Windows hosts, execute 'Get-WmiObject -Class

Win32_Product | Select-Object Name,Version | Export-Csv software_inv.csv' via PowerShell remoting. Schedule this as a weekly cron/Task Scheduler job. Two-person team: one runs external scans, one reconciles results against known asset list and flags delta systems with unpatched critical CVEs using the NVD feed (https://nvd.nist.gov/vuln/data-feeds).

**Evidence:** Before modifying any system configurations, preserve the current internet exposure baseline: export firewall/NAT rules and security group policies to document which ports and services are actively permitted inbound. Capture DNS zone records and public-facing hostnames via 'dig axfr' or zone transfer if accessible, or enumerate via passive DNS. Screenshot or export current cloud security group and load balancer listener configurations. This baseline documents the pre-directive exposure surface — critical for the CERT-In audit trail showing what was exposed and when remediation began, particularly if a vulnerability is later found to have been exploited during the gap window.

**Step 2: Process gap assessment — Compare your current vulnerability remediation SLAs against the 12-hour window for internet-facing critical vulnerabilities. Document which systems, teams, and approval workflows would block compliance with this timeline. Reference NIST SI-4 (System Monitoring) for continuous visibility requirements and CIS 7.1 (Establish and Maintain a Vulnerability Management Process) for process baseline.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: IR Plan Development and Process Readiness Assessment

**Controls:** CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST SI-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST IR-1 (Incident Response Policy and Procedures)

**Compensating:** Document current SLA gaps using a simple risk register spreadsheet with columns: Asset Name, External IP/FQDN, Software/Service, Current Patch SLA (days), CERT-In Required SLA (12 hours), Gap (Y/N), Blocking Workflow (CAB/Approver Name), Compensating Control Available (Y/N). For change approval bottlenecks, draft a pre-authorized emergency change template referencing the CERT-In directive citation so approvers can sign once rather than per-incident. A two-person team can complete this gap matrix in 4-6 hours using the nmap output from Step 1 combined with CVE data pulled from 'https://services.nvd.nist.gov/rest/json/cves/2.0' filtered on CVSS >= 9.0.

**Evidence:** Preserve the current state of your change management and patch records before beginning any process changes: export the last 90 days of change tickets (ServiceNow, Jira, or equivalent) for internet-facing assets to document historical time-to-patch metrics. This establishes a baseline for demonstrating improvement to CERT-In auditors and identifies which asset classes have historically exceeded 30-day remediation windows — those represent the highest regulatory exposure under the new 12-hour mandate. If a breach later occurs on a known-unpatched system, this record will be central to the regulatory inquiry timeline.

**Step 3: Detection and monitoring — Deploy continuous monitoring on internet-facing assets to detect active scanning and exploitation attempts. Log authentication events, service access, and anomalous outbound connections per NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting). Enable alerting on T1595.002-relevant indicators: high-rate scan traffic, automated user-agent strings, and sequential port probing against exposed services.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring, Indicator Collection, and Triage

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1595.002 (Reconnaissance: Vulnerability Scanning)

**Compensating:** Deploy Sysmon (SwiftOnSecurity config baseline) on all internet-facing Windows hosts to capture Event ID 3 (Network Connection) for unexpected outbound connections initiated by web-facing processes (IIS, Apache, Tomcat, nginx). On Linux hosts, use 'auditd' with rules targeting execve syscalls from web server user contexts (www-data, apache, nginx). At the network perimeter, run 'tcpdump -i eth0 -w /captures/scan_$(date +%F_%H%M).pcap "tcp[tcpflags] & tcp-syn != 0"' during business hours to capture SYN-scan patterns characteristic of AI-automated vulnerability scanners (Shodan, Nuclei, Interactsh callbacks). Deploy the free Suricata IDS with the ET Open ruleset — specifically rules in the 'SCAN' and 'EXPLOIT' categories — on a network tap or span port in front of

internet-facing segments. Alert thresholds: >500 unique port hits from a single source IP within 60 seconds is consistent with AI-accelerated scanning tooling.

**Evidence:** Before tuning detection rules, capture and preserve a 24-hour baseline pcap of normal traffic patterns to each internet-facing service so that AI-scanner traffic signatures (sequential port probing, non-browser user-agents like 'python-requests', 'nuclei', 'Nmap Scripting Engine', 'masscan') can be distinguished from legitimate traffic. Export current web server access logs (Apache: '/var/log/apache2/access.log'; nginx: '/var/log/nginx/access.log'; IIS: 'C:\inetpub\logs\LogFiles\') and WAF logs with timestamps intact — these pre-monitoring logs may already contain evidence of reconnaissance against your assets that preceded the CERT-In directive and are needed to establish whether exploitation preceded or followed disclosure of any specific CVE.

**Step 4: Remediation acceleration — Establish an emergency patch track for internet-facing critical vulnerabilities with pre-approved change authority, eliminating standard change advisory board delays for this asset class. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for automation targets. Where patching within 12 hours is operationally infeasible, document a compensating control — such as WAF rule deployment, temporary service isolation, or virtual patching — as an interim measure.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment: Short-Term Containment and Evidence Preservation During Active Risk

**Controls:** CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process), NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST IR-4 (Incident Handling)

**Compensating:** For teams without enterprise patch management (WSUS, Ansible, or Intune), use 'unattended-upgrades' on Debian/Ubuntu or configure 'yum-cron'/'dnf-automatic' with 'apply_updates = yes' scoped to security updates only, triggered immediately rather than on the default nightly schedule. For WAF-based virtual patching without budget: deploy ModSecurity (free, open-source) with the OWASP Core Rule Set (CRS) in front of vulnerable web services as an interim measure — this can be stood up in under 2 hours. For application isolation, use host firewall rules: 'iptables -I INPUT -p tcp --dport -j DROP' as an immediate containment measure while patching proceeds. Document every compensating control with: timestamp of deployment, specific CVE or vulnerability being mitigated, tool/rule deployed, and the CERT-In directive reference — this documentation is your regulatory defense if audited.

**Evidence:** Before applying any patch, take a snapshot or image of the affected internet-facing system (VMware snapshot, AWS AMI, or 'dd' image of critical partitions) to preserve forensic state. This is required under NIST 800-61r3 §3.3 containment guidance — patching without imaging first destroys potential evidence of pre-patch compromise. Specifically for the AI-accelerated exploitation context: capture active network connections ('ss -antp' on Linux; 'netstat -anob' on Windows), running process list with parent-child relationships ('ps auxf' on Linux; Sysmon Event ID 1 logs on Windows), and all recently modified files in web root directories ('find /var/www -newer /tmp/baseline_marker -ls') to detect web shells or implants that may have been installed during the window between vulnerability disclosure and patch deployment.

**Step 5: Post-directive hardening — Use this mandate as a forcing function to reduce internet exposure surface. Decommission or segment services that do not require public accessibility per CISA Internet Exposure Reduction Guidance. Apply D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) to all remaining internet-facing administrative interfaces. Document control gaps identified during scope assessment and assign remediation owners with tracked deadlines per NIST AC-6 (Least Privilege) and CIS 6.3 (Require MFA for Externally-Exposed Applications).**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned, Control Improvement, and Intelligence Sharing

**Controls:** NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.4

(Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** For MFA on internet-facing admin interfaces without commercial tooling: deploy Authelia (open-source, self-hosted) or enable TOTP-based MFA via PAM ('libpam-google-authenticator') for SSH on Linux hosts — setup time under 1 hour per host. To identify and decommission unnecessary internet-exposed services, run 'nmap --script=banner -p 1-65535 ' and compare against an approved services list; any service not on the approved list gets an immediate firewall DROP rule. For access review without enterprise IAM: export local admin group membership on all internet-facing Windows hosts via 'Get-LocalGroupMember -Group Administrators | Export-Csv admins_$(date +%F).csv' and review against HR roster — remove any account not actively required. Schedule this review monthly via Task Scheduler as a CERT-In compliance artifact.

**Evidence:** Post-hardening, capture and archive the following as your CERT-In compliance evidence package: (1) final nmap scan output showing reduced attack surface versus pre-directive baseline, (2) firewall rule export showing decommissioned or segmented services, (3) MFA enrollment report for all remaining internet-facing admin interfaces, (4) signed remediation ownership register mapping each control gap to a named owner and tracked deadline, and (5) the 90-day patch SLA historical export from Step 2 alongside the new emergency patch track SOP — together these demonstrate both the gap acknowledged and the process change made, which is the evidentiary standard CERT-In auditors will expect during a compliance review following any future incident.

## Detection Guidance

No specific IOCs are associated with this directive. Detection posture should focus on two areas: (1) Compliance visibility, maintain continuous asset discovery to identify newly exposed internet-facing services (CIS 1.1, CIS 1.2). Query your asset management and network perimeter tools weekly for services not in the authorized internet-exposure inventory. (2) Exploitation precursor activity, monitor for T1595.002 indicators on internet-facing assets: abnormally high connection rates from single IPs or ASNs, automated scanning signatures in web server and firewall logs, and sequential probing of service ports. For T1190, monitor application logs for malformed input patterns, unexpected authentication failures (NIST AU-2), and error spikes that may indicate automated exploit attempts. NIST AU-6 requires regular audit record review; configure SIEM alerts for scan-volume thresholds and anomalous service errors on perimeter assets. Where a CERT-In advisory references a specific CVE in the future, correlate against CISA's Known Exploited Vulnerabilities catalog and EPSS scores to triage prioritization.

## Framework Mappings

### MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1595.002** — Vulnerability Scanning

### NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-5** — Incident Monitoring

### CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

### NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1190 | Exploit Public-Facing Application | Initial-Access |
| T1595.002 | Vulnerability Scanning | Reconnaissance |

## Sources

| Source | URL | Tier |
|---|---|---|
| **gemini** | https://thehackernews.com/2026/05/cert-in-recommends-12-hour-patchi... | T3 |
| **Internet Exposure Reduction Guidance \| CISA** | https://www.cisa.gov/resources-tools/resources/exposure-reduction | T1 |
| **Understand How Internet Exposure Impacts Vuln Management** | https://nucleussec.com/blog/understand-internet-exposure-vuln-manag... | T3 |
| **Internet Exposure and Vulnerability Risk - Nucleus Security - YouTube** | https://www.youtube.com/watch?v=CygeqcTuJsk | T3 |
| **identify and prioritize internet-exposed services - Patrowl.io** | https://patrowl.io/en/blog/internet-exposed-services-security-mistakes | T3 |

Generated 2026-05-27 14:08 UTC by TJS Security Command Center