Guidelines regarding AI-Accelerated Vulnerability Protection and Response Requirements for Original Equipment Manufacturers (OEMs), and Technology Providers

Issued by:

V 1.0 | 10th June 2026

1. Introduction

India's rapidly expanding digital ecosystem, increasing interconnectivity of critical systems, cloud adoption, AI-enabled services, and growing dependence on software-driven infrastructure have significantly increased the cybersecurity risk landscape across sectors. Organizations across government, public sector, digital public infrastructure, telecommunications, banking, healthcare, manufacturing, transportation, digital services, and enterprise ecosystems are increasingly exposed to advanced cyber threats leveraging Artificial Intelligence (AI) and automated exploitation techniques.

Recent cybersecurity incidents globally, including misuse of AI models, AI-assisted vulnerability discovery, automated exploit generation, credential compromise, and accelerated attack execution capabilities, have fundamentally altered the cyber threat landscape. Threat actors are increasingly using AI-enabled tools to rapidly identify exploitable weaknesses, bypass traditional security controls, automate reconnaissance, and scale cyberattacks against digital infrastructure and supply chains. In this regard, Indian Computer Emergency Response Team (CERT-In) has issued an advisory titled "Defending Against Frontier AI Driven Cyber Risks" on 26 April 2026, for necessary mitigation actions.

Further, in view of the evolving threat environment, CERT-In is issuing enhanced cybersecurity compliance guidelines / recommendations for all global / domestic Original Equipment Manufacturers (OEMs), and technology provider (including software vendors, hardware manufacturers, cloud service providers, managed service providers, system integrators, technology partners, and digital service providers supplying products, software, firmware, platforms, cloud services, applications, APIs, or managed services) organizations operating in India.

2. Security Compliance Requirements

All OEMs and technology providers are advised to establish and maintain comprehensive cybersecurity governance, vulnerability management, and secure

product development practices for all products, software, firmware, cloud services, APIs, and digital platforms supplied to Indian organizations.

OEMs and technology providers should conduct comprehensive vulnerability assessments of all products and systems using both traditional security testing methodologies and AI-assisted vulnerability discovery techniques which include leveraging Machine Learning, LLMs, skills files, reasoning and automated testing to identify vulnerabilities. Security testing should include source code analysis, software composition analysis, dependency risk analysis, threat modelling, penetration testing, behavioural anomaly detection, and continuous security monitoring wherever feasible.

Organizations should also assess risks arising from the deployment and use of AI-enabled services, APIs, plugins, automation tools, and AI-assisted operational environments. Risk assessment should be conducted based on the key parameters such as Data sensitivity, Autonomy, Connectivity and Impact. Appropriate guardrails and safeguards such as human oversight, monitoring & logging, dependencies review (for details refer to chapter 12 of Reference [3], Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure) should be implemented to prevent misuse of AI systems for prompt injection, automated exploitation, malicious code generation, credential theft, unauthorized access, privilege escalation, social engineering, or data leakage.

OEMs and technology providers should maintain updated inventories (Bill of Material) of deployed products, software versions, exposed services, APIs, cryptography, third-party libraries, and associated software dependencies to support rapid vulnerability assessment and remediation activities. The Bill of Material for hardware / software / cryptography / AI / quantum should also be provided to the Indian customers including CERT-In, and updated on a regular basis.

2.1 Specific Obligations

a) Continuous Vulnerability Assessment Reports

OEMs and technology providers should setup continuous vulnerability assessment mechanism on deployed products and platforms.

b) Immediate Disclosure of Critical and High-Severity Vulnerabilities

Any Critical (CVSS 9.0–10.0) or High (CVSS 7.0–8.9) severity vulnerability affecting deployed systems, products, software, firmware, cloud services, or APIs should be communicated to affected organizations and CERT-In immediately upon discovery or confirmation, along with interim mitigation guidance and recommended remediation timelines.

c) Zero-Day Vulnerability Protocol

If an OEM or technology provider becomes aware of any zero-day vulnerability, active exploitation activity, or exploitation through AI-assisted techniques affecting deployed products or services, affected organizations including CERT-In should be notified immediately. Interim safeguards, temporary mitigation measures, indicators of compromise (IOCs), detection guidance, and recommended containment procedures should also be provided without delay.

d) AI-Assisted Security Testing Certification

OEMs and technology providers should maintain evidence and periodic certification confirming that security assessments including AI-assisted code analysis, automated vulnerability discovery mechanisms, security token scanning, dependency analysis, and advanced security validation using industry-recognized tools and methodologies have been carried out.

3. Accelerated Patch Management and Deployment

OEMs and technology providers should establish accelerated patch management and vulnerability remediation processes aligned with the evolving threat landscape and increasing speed of AI-assisted cyber exploitation.

Immediately upon identification or confirmation of a vulnerability, OEMs and technology providers should initiate technical validation, exploitability analysis, affected version identification, attack surface assessment, and risk evaluation activities. OEMs and technology providers should determine whether vulnerabilities

are remotely exploitable, internet exposed, privilege escalation capable, or actively weaponized in the wild.

3.1 Patch Development and Compensatory Controls Indicative Timelines

Vulnerability Categorization	Vulnerability discovered could likely be exploited using AI		Identified or Reported Vulnerabilities through Responsible Vulnerability Disclosure	
	Information Technology (IT)	Operational Technology (OT)	Information Technology (IT)	Operational Technology (OT)
Critical (CVSS 9.0–10.0)	Emergency Release	7 -15 Days	5 Days	15 -30 days
High (CVSS 7.0–8.9)	7 Days	15- 30 Days	15 Days	30-60 Days
Medium (CVSS 4.0–6.9)	14 Days	30- 60 Days	30 Days	60-90 Days

The indicative timelines should be implemented in conjunction with appropriate validation, testing, change management, and deployment procedures to ensure that remediation measures do not adversely impact the security, stability, safety, or operational continuity of Information Technology (IT) and Operational Technology (OT) environments.

Where immediate patch deployment is not feasible, OEMs and technology providers should provide interim mitigation guidance including:

- virtual patching mechanisms and compensatory security controls, ensuring minimal impact on operational continuity and service availability.
- disabling vulnerable services or features,
- network segmentation / micro-segmentation,
- firewall or IPS rule implementation,
- restriction of internet exposure,
- enhanced logging and monitoring,
- enforcement of multi-factor authentication,
- application allow-listing,

- temporary configuration hardening measures.

3.2 Patch Deployment Support

OEMs and technology providers should provide detailed patch deployment documentation, testing guidance, rollback procedures, validation mechanisms, compatibility considerations, operational impact assessment, and technical support during deployment activities. Validation scripts or integrity verification mechanisms should also be provided wherever applicable.

3.3 Automated Patch Notification

OEMs and technology providers should establish automated vulnerability and patch notification mechanisms to alert CERT-In and affected Indian organizations immediately when security advisories, mitigations, patches, or emergency remediation measures become available.

4. Secure Development Lifecycle (SDL) Compliance

OEMs and technology providers should implement and maintain industry-standard Secure Development Lifecycle (SDL) practices across all stages of product and software development.

SDL practices should include secure architecture reviews, secure coding standards, threat modelling, source code analysis, dynamic security testing, penetration testing, dependency validation, software composition analysis, supply chain risk management, secrets management, and security validation prior to release.

OEMs and technology providers should ensure that products are free from hardcoded credentials, insecure default configurations, exposed administrative interfaces, unsupported third-party libraries, debug mechanisms, or insecure authentication controls.

All software releases, firmware updates, security patches, APIs, and cloud components should undergo security validation prior to deployment or customer release.

OEMs and technology providers are also advised to maintain updated Software Bill of Material (SBOM) for products and software components to support vulnerability tracking and supply chain security management.

5. Credential and Access Management

OEMs and technology providers should implement robust credential, identity, and privileged access management controls across products, applications, support infrastructure, cloud environments, and administrative interfaces.

The use of hardcoded credentials, embedded secrets, default passwords, insecure API keys, or undocumented administrative access mechanisms should be strictly avoided.

OEMs and technology providers should implement:

- multi-factor authentication (MFA),
- role-based access control (RBAC),
- privileged access management,
- password rotation mechanisms,
- just-in-time privileged access,
- time-bound administrative access,
- continuous authentication monitoring,
- automated security token scanning across code repositories.

OEMs and technology providers should also conduct periodic credential hygiene audits and maintain evidence confirming that no customer-related credentials or secrets are exposed in public repositories, support systems, or unauthorized environments.

6. Incident Response and Transparency

OEMs and technology providers should establish formal cybersecurity incident response and vulnerability disclosure processes to support timely detection, containment, mitigation, recovery, and customer coordination during cybersecurity incidents. The same should be communicated in written to customers in India and to CERT-In.

Immediately upon discovery of active exploitation, compromise, or security incidents affecting deployed products or services, OEMs and technology providers should:

- initiate incident response procedures,
- notify affected organizations,
- preserve logs and forensic evidence,
- identify indicators of compromise (IOCs),
- assess operational and security impact,
- provide containment and recovery guidance,
- coordinate remediation and monitoring activities

As per directions issued by CERT-In under Section 70B of the Information Technology (Amendment) Act, 2008, vide CERT-In Directions No. 20(3)/2022-CERT-In dated 28 April 2022, cyber incidents are required to be reported to CERT-In within 6 hours of noticing such incidents or being informed about them.

6.1 Recommended Incident Notification Timelines

- Immediate internal escalation upon confirmation of critical security incidents.
- Preliminary incident notification to affected Indian organizations at the earliest possible stage with a copy to CERT-In.
- Detailed incident analysis including root cause, forensic findings, exploitation details, remediation status, and preventive measures should be shared as soon as reasonably practicable.
- In cases involving customer data compromise, credential exposure, ransomware, supply chain compromise, AI-assisted exploitation, or unauthorized administrative access, OEMs and technology providers should

provide regular status updates to their India customers and CERT-In until remediation and recovery activities are completed.

OEMs and technology providers should also ensure availability, integrity, synchronization, and secure retention of relevant logs and digital evidence including firewall logs, VPN logs, authentication logs, endpoint telemetry, cloud logs, network traffic logs, administrative activity logs, and security monitoring records to support incident investigation and forensic analysis.

7. Actionable Deliverables Required from OEMs and technology providers

Deliverable 1: Current Security Posture Assessment

OEMs and technology providers should maintain updated security posture assessments covering deployed products, software inventories, known vulnerabilities, CVSS severity scores, patch status, exposed attack surfaces, AI-related risks, exploitation exposure, and mitigation measures. The assessment should also include AI-assisted testing readiness, SDL compliance status, and credential hygiene verification.

Deliverable 2: Vulnerability Remediation Action Plan

OEMs and technology providers should maintain documented remediation plans containing:

- CVE identifiers,
- CVSS severity ratings,
- affected product versions,
- exploitation prerequisites,
- patch availability status,
- interim mitigation measures,
- testing requirements,
- deployment timelines,
- rollback procedures,

- operational impact considerations

Deliverable 3: Enhanced Security Compliance Commitment

OEMs and technology providers should provide formal security compliance commitments from their senior management confirming implementation of vulnerability management, secure development, incident response, patch management, logging, monitoring, and cybersecurity governance practices. OEMs and technology providers should also designate cybersecurity liaison officers and escalation contacts for incident coordination.

Deliverable 4: Continuous Security Assessment and Assurance Report

OEMs and technology providers should conduct continuous security assessments, including Vulnerability Assessment and Penetration Testing (VAPT), Breach and Attack Simulation (BAS), configuration reviews, and independent security audits. Updated reports should be maintained covering vulnerability status, remediation progress, penetration testing observations, security advisories, exposure analysis, unresolved risks, validation of security controls, compliance certifications, and updated Software Bill of Materials (SBOM) documentation to support security assurance, operational resilience, and risk management activities.

Deliverable 5: SDL Compliance Certification

OEMs and technology providers should maintain certification and evidence demonstrating compliance with Secure Development Lifecycle practices including code review, penetration testing, dependency management, security token management, patch validation, supply chain security controls, and secure release management.

8. Compliance Verification and Enforcement

8.1 Organization Verification Rights

Indian organizations including CERT-In, may conduct independent security assessments, vulnerability verification, patch validation, penetration testing, configuration reviews, and compliance verification activities for OEM / technology providers - supplied products, software, services, APIs, and infrastructure.

Indian organizations including CERT-In, may request additional documentation, security evidence, remediation status reports, incident response records, audit reports, SDL compliance documentation, SBOM details, or technical clarification whenever required.

Indian organizations including CERT-In, may also engage independent security testing agencies or third-party auditors to validate OEM security controls, patch effectiveness, vulnerability remediation status, and compliance posture.

For reporting of vulnerabilities, security incidents, disclosure coordination, submission of security assessment reports, or any clarification regarding these guidelines, OEMs and technology providers may coordinate with CERT-In at **oem.security@cert-in.org.in**

References

i. CERT-In Directions No. 20(3)/2022-CERT-In dated 28 April 2022 issued under Section 70B of the Information Technology Act, 2000

ii. Defending Against Frontier AI Driven Cyber Risks https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2026-0020

iii. Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure https://cert-in.org.in/PDF/Blueprint_for_Defending_against_AI_Assisted_Exploitataion.pdf