Science & Technology · GS - III

Software vulnerabilities pose a growing threat to India’s digital infrastructure. Examine the challenges and suggest measures to strengthen cybersecurity.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 23/10/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Software vulnerabilities, CERT-In, security patches, RCE, DoS, cyber resilience, incident response.

Model Answer

Introduction:

Increasing dependence on digital services has made software vulnerabilities a significant cybersecurity concern.

Main Body:

Challenges

1. Remote Code Execution: Vulnerabilities may allow attackers to run malicious code on affected systems.
2. Service Disruption: DoS attacks can interrupt websites and essential digital services.
3. Delayed Updates: Outdated software and unpatched systems increase exposure to cyberattacks.
4. Supply-Chain Risks: A vulnerability in widely used software can affect many organisations simultaneously.

-

Measures

1. Apply security patches promptly and maintain updated software inventories.

2. Conduct regular vulnerability assessments and penetration testing.
3. Strengthen incident reporting, threat monitoring and response mechanisms through CERT-In.
4. Promote secure software development, employee awareness and coordinated disclosure of vulnerabilities.

Conclusion:

A proactive, patch-driven and risk-based cybersecurity strategy is essential to protect India’s digital infrastructure and strengthen cyber resilience.

BECOME IAS
AI POWERED UPSC PREP