CERT-In warns of AI-assisted attacks causing unauthorized payments at Indian financial firms



India's CERT-In says attackers are using AI to target ICT assets, leading to unauthorized financial transactions at banks, financial services entities and technology providers.

- CERT-In, India's national computer emergency response team, issued the warning.
- Attackers are using AI-assisted techniques against ICT assets in the country.
- The activity has produced unauthorized financial transactions.
- Affected sectors include banking, financial services and technology service providers.

What was reported

India's national computer emergency response team, CERT-In, has warned that threat actors are carrying out

cyberattacks assisted by artificial intelligence against information and communication technology (ICT) assets in the country.

According to the report, this activity has led to unauthorized financial transactions at banking and financial services entities, as well as at technology service providers.

What the source does not say

The excerpt available to us does not name affected institutions, give amounts, or describe the specific techniques, vulnerabilities or tools involved. We have therefore not drawn conclusions on those points. Readers should consult the original CERT-In communication for technical detail as it becomes available.

Why it matters for Saudi institutions

The reported impact on both financial institutions and their technology providers is a reminder that payment fraud risk extends through the supply chain. Regulated institutions in the Kingdom may wish to use this warning as a prompt to re-test controls that protect payment initiation and approval, and to confirm that their providers can detect and report abnormal activity quickly.

No action is needed beyond prudent review at this stage, but the review is inexpensive relative to the exposure.

What to do now

1. Re-test approval workflows and limits for payment initiation, including out-of-band confirmation for high-value or unusual transactions.
2. Review monitoring rules for abnormal transaction patterns and confirm alerts reach the response team promptly.
3. Ask technology service providers how they detect and notify you of suspicious activity affecting your payment environment.
4. Check that incident response playbooks cover unauthorized payments and include contacts at SAMA and the NCA.