

## **Seqrite flags AI-driven zero-day exploitation risks for enterprises**

Cybersecurity firm Seqrite issues a stark warning. Advanced AI models can now find and exploit software flaws in hours, not months. This poses a significant threat to banks and financial institutions. India has already seen millions of cyber threats. Organizations must adopt proactive defenses. Faster patching and AI-driven threat detection are crucial.

Seqrite has issued an advisory to enterprises and financial institutions following the public disclosure of Anthropic's Claude Mythos AI model, warning that advanced AI systems could change how vulnerabilities are discovered and exploited.

According to the advisory, AI models such as Claude Mythos can autonomously identify and potentially weaponise zero-day vulnerabilities in critical software infrastructure. This could sharply reduce the time between vulnerability discovery and exploitation, from months to hours.

The advisory also points to Anthropic's Project Glasswing, a defensive initiative focused on identifying and addressing AI-discovered vulnerabilities. Seqrite warned that if similar capabilities become available through unregulated or open-weight AI models, malicious actors could use them to launch automated attacks at machine speed and scale.

Seqrite said this development is especially relevant for sectors such as banking and financial services, where complex infrastructure, third-party dependencies and sensitive data create a larger attack surface.

Citing findings from the India Cyber Threat Report 2026, the advisory noted that India has already recorded 265.52 million detections across more than 8 million endpoints, with threats increasingly linked to automation, AI-assisted phishing and identity compromise. Combined with advanced AI capabilities, this could enable vulnerabilities to be discovered, weaponised and deployed in near real time.

The advisory said organisations need to move beyond reactive security models and adopt more predictive, intelligence-led defence. This includes continuous vulnerability assessment, faster patching, AI-driven threat correlation, zero-trust identity frameworks, secure coding practices and real-time anomaly detection.

Seqrite also said existing incident response plans should be updated to account for AI-driven attacks that can identify and exploit zero-day vulnerabilities at scale. It recommended that enterprises reduce patching timelines for critical internet-facing vulnerabilities, reassess vendor and open-source dependency risks, and strengthen monitoring across identity, network and application layers.

The advisory suggests that AI-driven vulnerability discovery will become a major factor in enterprise cyber risk, making speed, visibility and resilience critical to future security strategies.