

Weekly threat recap: zero-days, rogue AI agents and trusted-service abuse



The Hacker News weekly recap points to 98 zero-days, rogue AI agents, a \$100M crypto theft and 700 supermarkets hit, with trusted services and devices as entry points. The excerpt gives few details.

- The recap headline cites 98 zero-days, rogue AI agents, a \$100M crypto theft and 700 supermarkets hit.
- The source says serious problems often arrive through trusted services, purchased devices or unchecked systems.
- It notes that trusted connections became a risk and hardware proved less safe than it appeared.
- Old vulnerabilities reportedly found new victims during the week.
- The available excerpt gives no technical detail, vendor names or CVE numbers.

The Hacker News published its weekly recap with a headline listing 98 zero-days, rogue AI agents, a \$100M crypto theft and 700 supermarkets hit. The excerpt available to us is short, so this item reflects only its general message.

What the recap says

The central theme is that the worst problems rarely announce themselves. They can arrive through a service everyone trusts, a device someone bought, or a system nobody thought to check. By the time something looks wrong, the damage may already be done.

The source adds that trusted connections became a problem during the week, hardware was less safe than it looked, and old bugs found new victims.

What is not known

The excerpt does not name the affected vendors, products, CVE numbers or victims, and it does not explain how the AI agents misbehaved or how the supermarkets were affected. We therefore cannot say whether any specific environment in the Kingdom is exposed.

Why it matters

For regulated institutions the lesson is about assumptions: third-party connections, newly procured hardware, forgotten systems and unpatched older vulnerabilities all deserve the same scrutiny as internet-facing assets. Readers should consult the full recap and the original vendor advisories before acting on any specific item.

What to do now

1. Review third-party and vendor connections and confirm each is still needed, monitored and limited in access.
2. Check asset inventories for forgotten or unmanaged systems and newly procured hardware.
3. Confirm older known vulnerabilities are patched, not only the latest ones.
4. Read the full recap and the original vendor advisories to see whether any listed item touches your environment.
5. Review how any AI agents in use are permitted to act, and what logging and limits apply.