Weekly threat roundup: critical firewall flaws, rented banking trojans and token theft



The Hacker News's weekly roundup points to critical firewall flaws, rented banking trojans, a weaponized PDF and token theft. Its common thread is exposed credentials, old bugs still exploited and abused trust.

- The roundup headline lists critical firewall flaws, rented banking trojans, a weaponized PDF and token theft, plus 26 more stories.
- It describes a mix of skilled attacks and simple oversights, such as exposed passwords.
- Older vulnerabilities are reportedly still being exploited.
- Attackers borrow trust from familiar apps, websites and AI tools, and some use AI to work faster.
- The excerpt gives no vendor names, CVE numbers or victim details.

The Hacker News's latest ThreatsDay roundup covers 26 more stories beyond its headline items: critical firewall flaws, banking trojans offered for rent, a weaponized PDF and token theft. The excerpt available to us is brief, so this note reflects only what it states.

What the roundup describes

The editors characterise the week as a mix of clever techniques and careless mistakes. Some attacks demand real skill, while others succeed because something was simply left open. Exposed passwords, old bugs that are still being exploited, and trusted software behaving in ways it should not all feature.

A recurring theme is borrowed trust. Attackers lean on familiar apps, websites and AI tools to look legitimate, and some use AI to move faster.

What is not yet known

The excerpt does not name the affected firewall products, give CVE identifiers, or describe specific victims or fixes. We therefore cannot say which environments are exposed. Readers should consult the full article and the relevant vendor advisories before acting on any single item.

Why it matters

None of the themes is new, but together they are a useful reminder. Perimeter devices, identity and token handling, and routine document and software trust are everyday exposure points. Institutions can review these areas now without waiting for further detail.

What to do now

1. Read the full source article and identify which items apply to your firewall and software estate.
2. Check vendor advisories for your firewall products and confirm patch status, prioritising internet-facing devices.
3. Scan for exposed or reused passwords and enforce multi-factor authentication on remote and administrative access.
4. Review session and token lifetimes and alerting for anomalous sign-ins.
5. Remind staff to treat unexpected PDF attachments with caution and test email filtering for them.