Unpatched Windows zero-day FastUnlock allows programs to run on a locked PC



A newly disclosed, unpatched technique called FastUnlock lets someone with physical access to a locked Windows PC start programs without signing in, though only under a limited account rather than administrator control.

- FastUnlock is a zero-day technique with no patch available at the time of the report.
- It requires physical access to a locked Windows computer.
- It allows programs to start without signing in.
- The attacker obtains only a limited account, not administrator control.
- The method was published by a researcher using the handles MSNightmare and Nightmare Eclipse; ThreatLocker is also named in the source.

What was disclosed

A researcher using the handles MSNightmare and Nightmare Eclipse has published a technique called **FastUnlock**. According to the report, it allows a person who is physically holding a locked Windows computer to start programs on it without signing in. The issue is unpatched, which makes it a zero-day.

What it does and does not allow

The access gained is limited. The person using the method obtains a limited account and not administrator control of the machine. The source excerpt does not describe the technical mechanism, the affected Windows versions, or any vendor response, so those points should not be assumed.

Why it matters

The risk applies mainly to devices that can be physically reached by unauthorised people: laptops taken on travel, devices left in shared spaces, and lost or stolen equipment. A limited foothold can still be a starting point for further steps, so physical security and device protection remain part of the defence. Teams should follow Microsoft's channels for any fix and review their exposure in the meantime.

What to do now

1. Monitor Microsoft's official channels for a patch or mitigation guidance and plan rapid deployment once available.
2. Identify Windows laptops and shared or public-area workstations where physical access by unauthorised people is realistic.
3. Reinforce physical safeguards: lock-away storage, cable locks, and clear rules against leaving devices unattended.
4. Confirm that lost or stolen device reporting and remote lock or wipe procedures work and are known to staff.
5. Ensure full-disk encryption and least-privilege accounts are enforced so a limited foothold has little value.