Windows Hello vulnerability allows hackers to log in with fake facial photos

However, recently, at the Black Hat security conference in Las Vegas, two researchers Tillmann Osswald and Dr. Baptiste David (from Germany) revealed how the enterprise version of Windows Hello can be cracked, raising an extremely serious security issue.

Back in May, Microsoft started setting up new accounts **as passwordless by default** . Instead of typing in a password, the company encouraged users to switch to modern login methods like **Passkey** or **Windows Hello** .

However, recently, at the **Black Hat** security conference in Las Vegas, two researchers Tillmann Osswald and Dr. Baptiste David (from Germany) revealed how the enterprise version of Windows Hello can be cracked, raising an extremely serious security issue.

Direct 'infiltration'

Accordingly, in the demo, David logged into his computer using **facial recognition** . Then, Osswald – acting as a hacker with local admin rights – only needed to run a few lines of code. He inserted his facial scan (taken on another machine) into the target machine's **biometric database** . Just a few seconds later, Osswald put his face in front of the camera and… the computer unlocked immediately, mistaking Osswald's face for David's.

How Windows Hello works

When Windows Hello is first set up, the service generates **a public/private key pair** . The public key is registered with the organization's ID provider (such as Entra ID).

Biometric data (face, fingerprints, etc.) is stored in a database managed by **Windows Biometric Service (WBS)** , and this database is encrypted. When logging in, the system will match the live scan data with the saved template.

The problem is: in some cases, this layer of encryption **cannot prevent an attacker with local admin privileges** from decrypting and replacing biometric data.

To overcome this, Microsoft introduced **ESS** – an enhanced security feature that puts the entire biometric authentication process into **an isolated security environment** managed by the system's hypervisor.

But ESS only works when the machine meets the hardware requirements including:

1. New 64-bit CPU supports hardware virtualization (VBS)
2. TPM 2.0 Chip
3. Secure Boot enabled in BIOS/UEFI
4. Specially certified biometric sensors

Microsoft mandated this feature on the **Copilot+ PC** line , but many current machines don't have it, especially AMD-based PCs that don't have security camera sensors.

According to researchers Osswald and David, a complete fix is almost **impossible** without redesigning the entire biometric data storage architecture. Therefore, if you are using Windows Hello **without ESS** , they recommend **disabling biometrics completely** and switching to a PIN.

To check if your system supports ESS, go to **Settings > Accounts > Sign-in options** . If you see the option **'Sign in with external camera or fingerprint reader'** :

1. **Off** : ESS is active (but peripherals such as USB fingerprint will not be available).
2. **On** : ESS is disabled (external devices can be used but security is reduced).

Microsoft says some 'Windows Hello compatible' peripherals can enable ESS, but to be safe, they should be plugged in on first boot and not unplugged. Full support for external devices with ESS is not expected until **late 2025** .