Microsoft’s Windows Hello fingerprint authentication has been bypassed

Microsoft’s Windows Hello fingerprint authentication has been bypassed on laptops from Dell, Lenovo, and even Microsoft. Security researchers at Blackwing Intelligence have discovered multiple vulnerabilities in the top three fingerprint sensors that are embedded into laptops and used widely by businesses to secure laptops with Windows Hello fingerprint authentication.

Microsoft’s Offensive Research and Security Engineering (MORSE) asked Blackwing Intelligence to evaluate the security of fingerprint sensors, and the researchers provided their findings in a presentation at Microsoft’s BlueHat conference in October. The team identified popular fingerprint sensors from Goodix, Synaptics, and ELAN as targets for their research, with a newly-published blog post detailing the in-depth process of building a USB device that can perform a man-in-the-middle (MitM) attack. Such an attack could provide access to a stolen laptop, or even an “evil maid” attack on an unattended device.

A Dell Inspiron 15, Lenovo ThinkPad T14, and Microsoft Surface Pro X all fell victim to fingerprint reader attacks, allowing the researchers to bypass the Windows Hello protection as long as someone was previously using fingerprint authentication on a device. Blackwing Intelligence researchers reverse engineered both software and hardware, and discovered cryptographic implementation flaws in a custom TLS on the Synaptics sensor. The complicated process to bypass Windows

Hello also involved decoding and reimplementing proprietary protocols.

Fingerprint sensors are now widely used by Windows laptop users, thanks to Microsoft's push towards Windows Hello and a password-less future. Microsoft revealed three years ago that nearly 85 percent of consumers were using Windows Hello to sign into Windows 10 devices instead of using a password (Microsoft does count a simple PIN as using Windows Hello, though).

This isn't the first time that Windows Hello biometrics-based authentication has been defeated. Microsoft was forced to fix a Windows Hello authentication bypass vulnerability in 2021, following a proof-of-concept that involved capturing an infrared image of a victim to spoof Windows Hello's facial recognition feature.

It's not clear if Microsoft will be able to fix these latest flaws alone, though. "Microsoft did a good job designing Secure Device Connection Protocol (SDCP) to provide a secure channel between the host and biometric devices, but unfortunately device manufacturers seem to misunderstand some of the objectives," writes Jesse D'Aguanno and Timo Teräs, Blackwing Intelligence researchers, in their in-depth report on the flaws. "Additionally, SDCP only covers a very narrow scope of a typical device's operation, while most devices have a sizable attack surface exposed that is not covered by SDCP at all."

The researchers found that Microsoft's SDCP protection wasn't enabled on two of the three devices they targeted. Blackwing Intelligence now recommends that OEMs make sure SDCP is enabled and ensure the fingerprint sensor implementation is audited by a qualified expert. Blackwing Intelligence is also exploring memory corruption attacks on the sensor firmware and even fingerprint sensor security on Linux, Android, and Apple devices.

https://www.theverge.com/2023/11/22/23972220/microsoft-windows-hello-fingerprint-authentication-bypass-security-vulnerability