
***Issued 5/14/17***

**HP Laptops and Tablets Shipped with Audio Driver Acting as Keylogger**

It looks like many HP laptops and tablet PCs were shipped with a Conexant audio driver that can log keystrokes. This makes it a lot easier for any malicious actors to steal sensitive information from victims without even being detected. The discovery was made by security firm Modzero who noticed that MicTray64.exe, an app that comes with many HP devices alongside the Conexant audio driver package and that's registered as a scheduled task in Windows, is actually a keylogger.

The official purpose of this feature is to figure out if the user has pressed any of the audio-related keys in order to mute or unmute the computer, for instance. Now, if the only feature this tool came with was "monitoring" keystrokes, it wouldn't have been such a huge deal. However, those keystrokes are logged to a file in the Users/Public folder and passed on to the OutputDebugString debugging API. This allows a process to access the data via the MapViewOfFile function, the researchers point out. Long story short, a user's sensitive data, including those precious passwords, get logged by this tool and stored in an easily-accessible location.

With the right malware, all that data could get picked up quite easily without as much as triggering an alarm with the security product you may have on your device. “There is no evidence that this keylogger has been intentionally implemented. Obviously, it is a negligence of the developers - which makes the software no less harmful. If the developer would just disable all logging, using debug-logs only in the development environment,

there wouldn't be problems with the confidentiality of the data of any user," notes Thorsten Schroeder, security researcher with Modzero.

HP is already working on a fix for the problem and will soon roll it out to customers. The vulnerability affects 28 HP laptops and tablets.