Project Zero

News and updates from the Project Zero team at Google

```
[ Download | Text view ]
```

Ex-Man and the CS3 Expert Level

Posted by Ian Beer, Project Zero

TL;DR

This exploit provides evidence for three logical chains were likely written: vulnerabilities with the supposed CS3 sensors, that is, the exploit technique which would be required to exploit a vulnerability in the sensor driver, and a bug which would be required to trigger that exploit technique. This exploit is very unlikely to be a proof of concept.

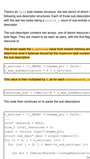
The end of the timeline for the sensor bug which exploit-wise are never actually used, that was directly inactivated from the hidden system menu.

Exploiting the Sensor Hub Firmware

```
[ Download | Text view ]
```

Ex-Man exploits a vulnerability in the sensor hub firmware, part of the Qualcomm Hexagon DSP, which is used to offload sensor processing from the application processor. Ex-Man uses the Qualcomm Hexagon DSP's shared memory interface to exploit the application processor.

Ex-Man's sensor hub exploit is written in the Qualcomm Hexagon DSP's assembly language and uses **Qualcomm's proprietary** RTOS. Ex-Man's sensor hub exploit also uses Qualcomm's proprietary shared memory protocol to communicate with the application processor. Ex-Man's sensor hub exploit uses proprietary shared memory protocols to exchange data with the application processor. Ex-Man's sensor hub exploit uses proprietary shared memory protocols to exchange data with the application processor. Ex-Man's sensor hub exploit uses proprietary shared memory protocols to exchange data with the application processor.


Qualcomm Hexagon DSP
Qualcomm Hexagon DSP Shared Memory Interface
Qualcomm Hexagon DSP Shared Memory Interface
Qualcomm Hexagon DSP Shared Memory Interface