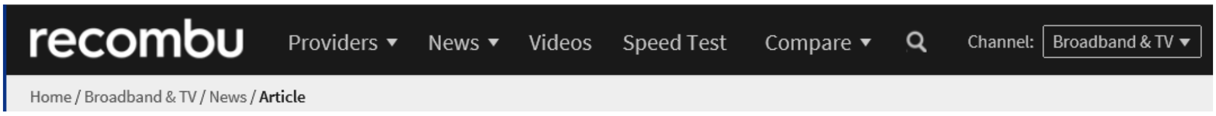

Panic! Hundreds of thousands of routers, cameras and other IoT devices have security holes

By Clare Hopping

Monday, 25th August 2014

Smart home tech has been labelled a security disaster in a huge test which found gaping holes in hundreds of thousands of connected devices.

Researchers in France found more than 140,000 Internet of Things (IoT) devices, from routers to CCTV systems can be hacked, allowing criminals to find out information about you and your network.

Eurecom also found problems in the apps that control the hardware, with one major vendor's application giving hackers 'back-door' access to your smart home system - it's available on Google Playand has half a million users.

It's not just the governments watching you - hackers are too, though your smart CCTV system

The company said: "Whenever a new vulnerability was discovered our analysis infrastructure allowed us to quickly find related devices or firmware versions that were likely affected by the same vulnerability."

This means if a problem was found on one device, it could easily be matched up to find others from the same manufacturer, or even different brands using the same components and firmware.

Eurecom said manufacturers are allowing too many easy-to-crack passwords, easily accessible private keys and 'zero-day' vulnerabilities. Zero-day vulnerabilities are problems that go unnoticed by engineers, but if uncovered by hackers can be used with no defence.

Eurecom found 38 previously unknown vulnerabilities in over 693 firmware images and reported that the problems were affecting at least 140,000 devices accessible over the Internet.

Earlier in the week, the BBC revealed its own research that showed baby monitors and webcams connected to the internet could allow virtual burglars to access information about your home.

Other reports, released in the last month show just how widespread the problems are, with HP's research claiming 70 per cent of IoT devices have security flaws and routers targeted at the Defcon 22 hacker conference, showing five widely-available home routers can be hacked faster than ever imagined due to outdated firmware.

Unfortunately, many reports into Internet of Things security flaws have refused to name the manufacturers whose kit fails their tests, either because they want to sell them the information, or because they're concerned about legal action.