Issued 1/3/17

Security Flaws Put Virtually All Phones, Computers at Risk

Security researchers on Wednesday disclosed a set of security flaws that they said could let hackers steal sensitive information from nearly every modern computing device containing chips from Intel Corp, Advanced Micro Devices Inc and ARM Holdings. One of the bugs is specific to Intel but another affects laptops, desktop computers, smartphones, tablets and internet servers alike. Intel and ARM insisted that the issue was not a design flaw, but it will require users to download a patch and update their operating system to fix. “Phones, PCs, everything are going to have some impact, but it’ll vary from product to product,” Intel CEO Brian Krzanich said in an interview with CNBC Wednesday afternoon.

The first flaw, called Meltdown, affects Intel chips and lets hackers bypass the hardware barrier between applications run by users and the computer's memory, potentially letting hackers read a computer's memory and steal passwords. The second, called Spectre, affects chips from Intel, AMD and ARM and lets hackers potentially trick otherwise error-free applications into giving up secret information. The researchers said Apple Inc and Microsoft Corp had patches ready for users for desktop computers affected by Meltdown.

Microsoft declined to comment and Apple did not immediately return requests for comment. Daniel Gruss, one of the researchers at Graz

University of Technology who discovered Meltdown, called it "probably one of the worst CPU bugs ever found" in an interview with Reuters. It also reported [link] that the updates to fix the problems could causes Intel chips to operate 5 percent to 30 percent more slowly. Intel denied that the patches would bog down computers based on Intel chips. AMD chips are also affected by at least one variant of a set of security flaws but that it can be patched with a software update. The company said it believes there "is near zero risk to AMD products at this time." Google said in a blog post that Android phones running the latest security updates are protected, as are its own Nexus and Pixel phones with the latest security updates. Gmail users do not need to take any additional action to protect themselves, but users of its Chromebooks, Chrome web browser and many of its very time there is data transmitted over the Internet, irrespective of whether it's an email, Google Search or retail transaction, the data is broken down into digital information that is sent in data packets. The packets are labelled and addressed with instructions explaining where they are going to. Millions of data packets move between destinations all the time, uninterrupted," she said. "If someone has installed sniffing hardware or software somewhere on the network, they can eavesdrop, snatch that data in mid-transmission just long enough to 'sniff' or inspect it, and if found to be interesting or valuable, quickly capture and copy it before sending it on its way. This is done without anyone being the wiser. Packet sniffing is like wiretapping for the Internet." Packet sniffers can read emails, see passwords, view your Web history, and more alarmingly, capture account information such as logins and credit card numbers in detail. "Again, I recommend turning to strong encryption, in the form of a VPN to avoid this scourge," said Poorter. "Sidejacking, or session hijacking, is a method an attacker will use to essentially steal a user's access to a Web site by using a packet sniffer to get their hands on an unencrypted cookie that grants access to the site in question. Google Cloud services will need to install updates. Amazon Web Services, a cloud computing service used by businesses, said that most of its internet servers were already patched and the rest were in the process of being patched. The defect affects the so-called kernel memory on Intel x86 processor chips manufactured over the past decade, The Register

reported citing unnamed programmers, allowing users of normal applications to discern the layout or content of protected areas on the chips. That could make it possible for hackers to exploit other security bugs or, worse, expose secure information such as passwords, thus compromising individual computers or even entire server networks.

Dan Guido, chief executive of cyber security consulting firm Trail of Bits, said that businesses should quickly move to update vulnerable systems, saying he expects hackers to quickly develop code they can use to launch attacks that exploit the vulnerabilities. “Exploits for these bugs will be added to hacker’s standard toolkits,” said Guido.