Hacker posts confidential Intel specs online

August 7 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

Intel suffered a massive breach Thursday as 20 GB of internal documents were published online.

The confidential documents contain data on the internal designs of chipsets dating back to 2016.

The data were sent by an anonymous source to a Swiss software engineer, Till Kottmann, who specializes in uploading hacked documents. He does so, he has said, to encourage companies to exercise more caution concerning security and "to better find and assess potential issues." But he admits he is also motivated to release unauthorized documents obtained from hackers "to free information" for all to see.

The data were also posted to an online file-sharing web site.

The data dump contains sensitive files obtained from the Intel Resource and Design Center, which provides information for customers and corporate partners. The documents may be accessed only after users sign non-disclosure agreements.

It is not clear whether the anonymous source hacked their system or accessed it internally.

"We are investigating this situation," Intel said in a statement Thursday. "We believe an individual with access downloaded and shared this data."

For Intel, already going through a rough period as its market value plummeted by more than $40 billion following recent reports of yet another setback in production schedule for its 7nm chips and an internal reorganization that saw the ouster of its chief engineering officer, the breach may be just the tip of the iceberg.

According to Kottmann, this week's release is only the first part of a series of data dumps coming in the near future.

Topics of the confidential documents include such titles as "Binaries for Canera drivers Intel made for SPaceX," "Schematics, Docs, Tools and Firmware for the unreleased Tiger Lake platform," "Simics Simulation for Rocket Lake S and potentially other platforms" and "Bootguard

SDK."

The leak also contains technical specs and PDF presentations on Intel's upcoming Tiger Chip, slated for distribution starting next month.

Some observers were amused that among passwords Intel used on internal documents retrieved in data breach are the surprisingly weak "Intel123" and "I accept."

An Intel spokeswoman said it does not appear that and customer or personal information has been compromised. However, segments of BIOS code revealed in the dump cold potentially be used by hackers to reverse engineer a hack that could affect current or future Intel products.

Based on his communications with the hacker, Kottmann predicted the current leak is just one "in a series of large Intel leaks."

"Future parts of this leak," Kottmann tweeted, "will have even juicer and more classified stuff."

Also troubling was the anonymous hacker's assertion, made in a chat with Kottmann, that he could impersonate Intel employees.

"Due to a misconfiguration," the hacker said, "I could masquerade as any of [Intel's] employees or make my own user"name.

This latest breach recalls a 2017 episode in which confidential source code for Microsoft Windows 10, intended for "qualified customers, enterprises, governments, and partners for debugging and reference purposes," was leaked online.

More information:
twitter.com/deletescape/status/1291405688204402689