Audit: No Chinese surveillance implants in Supermicro boards found

Enlarge / A letter posted by Supermicro executives today announcing that an audit had found no evidence of claims of espionage implants in the company's servers, part of a campaign by the company to counter a report by Bloomberg in October.

reader comments

159 with 97 posters participating

Share this story

In a letter to customers issued December 11, Supermicro President and CEO Charles Liang and other top executives announced that an audit conducted by an outside investigating team had found no evidence of any malicious hardware incorporated into motherboards currently or previously manufactured by the company. The letter is the latest rebuttal to Bloomberg reports in October that claimed tiny chips that provided a backdoor for China's intelligence agencies had been integrated into boards provided to major Internet and cloud providers—a report also refuted by the companies the report claimed were targeted.

"After a thorough examination and a range of functional tests, the investigative firm found absolutely no evidence of malicious hardware on our motherboards," the letter signed by Liang, Supermicro Senior Vice President and Chief Compliance Officer David Weigland, and Senior VP and Chief Product Officer Raju Penumatcha stated. "These findings were no

surprise to us… We appreciate the industry support regarding this matter from many of our customers, like Apple and AWS. We are also grateful for numerous senior government officials, including representatives of the Department of Homeland Security, the director of National Intelligence, and the director of the FBI, who early on appropriately questioned the truth of the media reports."

Reuters' Joseph Menn reported that the audit was apparently undertaken by Nardello & Co, a global investigative firm founded by former US federal prosecutor Daniel Nardello. According to Reuters' source, the firm examined sample motherboards that Supermicro had sold to Apple and Amazon, as well as software and design files for products. No malicious hardware was found in the audit, and no beacons or other network transmissions that would be indicative of a backdoor were detected in testing.

The letter and an accompanying video detailed Supermicro's supply chain security procedures, including repetitive testing of products during manufacturing, oversight and inspection during manufacturing by Supermicro employees, compartmentalization of access to board design data across Supermicro (with no single employee having access to all of the design elements), and regular audits of suppliers. "The complexity of our motherboard design serves as an additional safeguard," the Supermicro executives wrote. Throughout our supply chain, each of our boards is tested repeatedly against its design to detect any aberration and to reject any board that does not match its design."

"As we have stated repeatedly since these allegations were reported, no government agency has ever informed us that it has found malicious hardware on our products," Supermicro's executives said. "No customer has ever informed us that it found malicious hardware on our products; and we have never seen any evidence of malicious hardware on our products. Today's announcement should lay to rest the unwarranted

accusations made about Supermicro’s motherboards.”

Bloomberg had reported that in addition to targeting Apple and Amazon Web Services, Chinese intelligence had managed to get implanted hardware inside an unnamed major telecommunications provider. The alleged victim was never named, with Bloomberg’s report citing a non-disclosure agreement signed by the company Bloomberg used as its source for the story, Sepio Systems. Sepio’s co-CEO, Yossi Appleboum, claimed that a scan had revealed the implant and that it had been added to an Ethernet adapter when the computer was manufactured.

https://arstechnica.com/?p=1426551