Security Advisory Report - Security Advisory Report - OBSO-1810-01

Chinese spy chips in Supermicro servers

Creation Date: 2018-10-08 18:08:50
Last Update: 2018-12-14 14:57:10

Summary

According to a Bloomberg report Chinese government agents managed to install spy chips in Supermicro servers which are used by Amazon, Apple, the US government and about 30 other organizations.

Unify products are not manufactured by Supermicro and thus are not affected.

Apple and Amazon state everything is false, no spy chip found on their boards.

Update:

On December 11th Supermicro CEO Charles Liang published an official letter to all it's customers informing that the external audit and thorough investigation of their products found no evidence of malicious hardware on their motherboards.

Read CEO Charles Liang's letter

This shows clearly, that there is no threat in Supermicro motherboards, no need for further actions.

Details

Bloomberg revealed that a Taiwanese/ US manufacturer of servers, Supermicro, which HQ is in San Jose has been compromised by China.

The hack works like this:

· The Supermicro server has a motherboard

· This motherboard included a small, well hidden chip produced by a Chinese manufacturer

· This chip is actually a Trojan horse allowing:

  · Establishment of a back tunnel to the server of the state-sponsored hacker in China

· Providing a script allowing this China server to control the Supermicro server

Not all Supermicro motherboards are affected, just those that have the Chinese spy chip.

For details see:

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

https://www.theregister.co.uk/2018/10/04/supermicro_bloomberg/

A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.

The compromised motherboards were built into servers assembled by Supermicro.

The sabotaged servers made their way inside data centers operated by dozens of companies.

When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.

Apple and Amazon state everything is false, no spy chip found on their boards.

https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

ars states there are easier ways to spy boards than impanting a chip.

https://arstechnica.com/information-technology/2018/10/supermicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants/

Recently there are some doubts about the Bloomberg report:

https://risky.biz/RB517_feature/

Affected Products

Unify products are not affected, they do not use Supermicro servers.

Recommended Actions

At the moment no activity is required.

References

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

https://www.theregister.co.uk/2018/10/04/supermicro_bloomberg/

https://risky.biz/RB517_feature/

https://www.heise.de/security/meldung/Bericht-Winzige-Chips-spionierten-in-Cloud-Servern-von-Apple-und-Amazon-4181461.html

https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

https://arstechnica.com/information-technology/2018/10/supermicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants/

https://fm4.orf.at/stories/2940104/

Advisory: Security Advisory Report - OBSO-1810-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com