RATTLED: CHINA'S HARDWARE HACK – AMAZON'S RESPONSE

[*NB: Note the byline. Portions of my analysis may be speculative. / ~Rayne*]

The following analysis includes a copy of an initial response received from Amazon by Bloomberg Businessweek in response to its story, The Big Hack. In tandem with the Bloomberg story Amazon's response was published on October 4 at this link. The text of Amazon's response is offset in blockquote format. No signer was indicated in the published response. Additional responses by Amazon to Bloomberg's story will be assessed separately in a future post.

This analysis is a work in progress and subject to change.

———————

Amazon

> It's untrue that AWS[1] knew about a supply chain compromise, an issue with malicious chips, or hardware modifications[2] when acquiring Elemental. It's also untrue that AWS knew about servers containing malicious chips or modifications in data centers based in China, or that AWS worked with the FBI[3] to investigate or provide data about malicious hardware.

[1] Identity – were there ever any third-party contractors or representatives involved in the relationship with Elemental? With Supermicro? Are there more than one Amazon subsidiary entity involved in the evaluation, purchasing, implementation of Elemental or Supermicro products into Amazon or its subsidiary enterprise? Which entity submitted this denial to Bloomberg Businessweek: Amazon, AWS, or some other subsidiary?

[2] What about evidence of bad or mismatched firmware and firmware updates?

[3] Did any law enforcement, military, or intelligence agency work with Amazon or any of its subsidiaries or contractors to investigate or provide data on hardware which failed to operate to specification or as expected?

> We've re-reviewed our records[4] relating to the Elemental acquisition for any issues related to SuperMicro, including re-examining a third-party security audit[5] that we conducted in 2015 as part of our due diligence prior to the acquisition. We've found no evidence to support claims of malicious chips or hardware modifications.[6]

[4] "our records" – whose records and what kind? Identity needs clarification as well as the type of records.

[5] Who is the third-party security auditor? How and why were they engaged?

[6] What about evidence of bad or mismatched firmware and firmware updates?

> The pre-acquisition audit described four issues with a web application (not hardware or chips)[7] that SuperMicro provides for management of their motherboards. All these findings were fully addressed before we acquired Elemental. The first two issues, which the auditor[8] deemed as critical, related to a vulnerability in versions prior to 3.15 of this web application (our audit covered prior versions of Elemental appliances as well), and these vulnerabilities had been publicly disclosed by SuperMicro on 12/13/2013.[9]

[7] "web application" – but not firmware?

[8] Is this still the unnamed third-party

security auditor or an internal auditor employed by Amazon or a subsidiary?

[9] How was this “publicly disclosed by SuperMicro”? SMCI’s website does not currently have either a press release or an SEC filing matching this date (see screenshots at bottom of this page).

> Because Elemental appliances are not designed to be exposed to the public internet, our customers are protected against the vulnerability by default.[10] Nevertheless, the Elemental team had taken the extra action on or about 1/9/2014 to communicate with customers and provide instructions to download a new version of the web application from SuperMicro (and after 1/9/2014, all appliances shipped by Elemental had updated versions of the web application).[11] So, the two “critical” issues that the auditor found, were actually fixed long before we acquired Elemental. The remaining two non-critical issues with the web application were determined to be fully mitigated by the auditors if customers used the appliances as intended, without exposing them to the public internet.[12]

[10] “exposed to the public internet” – did customer data run through Elemental’s Supermicro devices between 2013 and 2015?

[11] What about firmware?

[12] Did customer data still run through devices with the two non-critical issues? Are any machines with these non-critical issues still in production?

> Additionally, in June 2018, researchers made public reports of vulnerabilities in SuperMicro firmware.[13] As part of our standard operating procedure, we notified affected customers promptly,

> and recommended they upgrade the firmware in their appliances.[14]

[13] Researchers at Eclypsium are reported to have told Supermicro of vulnerabilities in January 2018. When was Amazon, AWS, or other Amazon subsidiary notified of these vulnerabilties?

[14] Give the six-month gap between Eclypsium's notification to Supermicro and the public's notification, when were Amazon's, AWS', or other Amazon subsidiary's customers notified of these vulnerabilties?

Screenshots

Supermicro's SEC filings – last of year 2013:

Supermicro's press releases – last of year 2013:


Home | Contact Us |
Search
About Us
Products
Solutions
Support
Newsroom
Where To Buy
About Supermicro®
About Home
Company Milestones
Investor Relations
Press Releases
Management
Events & Presentations
Corporate Governance
Financial Information
Stock Information
Contact Us
Green Computing
Careers
Contact
Policies
Investor Relations
Press Releases
Year:
2013
Items per page:
10
Supermicro® Expands Range of Energy Efficient VDI Server Solutions for NVIDIA GRID
Dec 11, 2013
Supermicro® 1U 4x GPU SuperServer® in Green500 #1 Ranked TSUBAME-KFC Supercomputer from Tokyo Institute of Technology (GSIC
Dec 3, 2013
Supermicro® Debuts Powerful 4U 8x GPU SuperServer® Optimized for the New NVIDIA Tesla K40 GPU Accelerator at Supercomputing 2013
Nov 18, 2013
Supermicro® Unveils New 2-Node 4U FatTwin™ Supporting 12x Intel® Xeon Phi™ Coprocessors and New TwinPro™ Platforms featuring 12Gb/s SAS 3.0 and NVMe at Supercomputing 2013
Nov 18, 2013
Supermicro® Unveils New 2-Node 4U FatTwin™ Supporting 12x Intel® Xeon Phi™ Coprocessors and New TwinPro™ Platforms featuring 12Gb/s SAS 3.0 and NVMe at Supercomputing 2013
Stock Information
SMCI (NASDAQ)
Oct 8, 2014
-- 0.00
Copyright Wall LLC.
Minimum 15 minutes delayed
Shareholder Tools
Printed Materials
Email Alerts
Download Library
RSS News Feeds
Print page
IR Information
IR at Supermicro
PH# 408-895-6570
Email
ir@supermicro.com
Search Investor Relations
Go