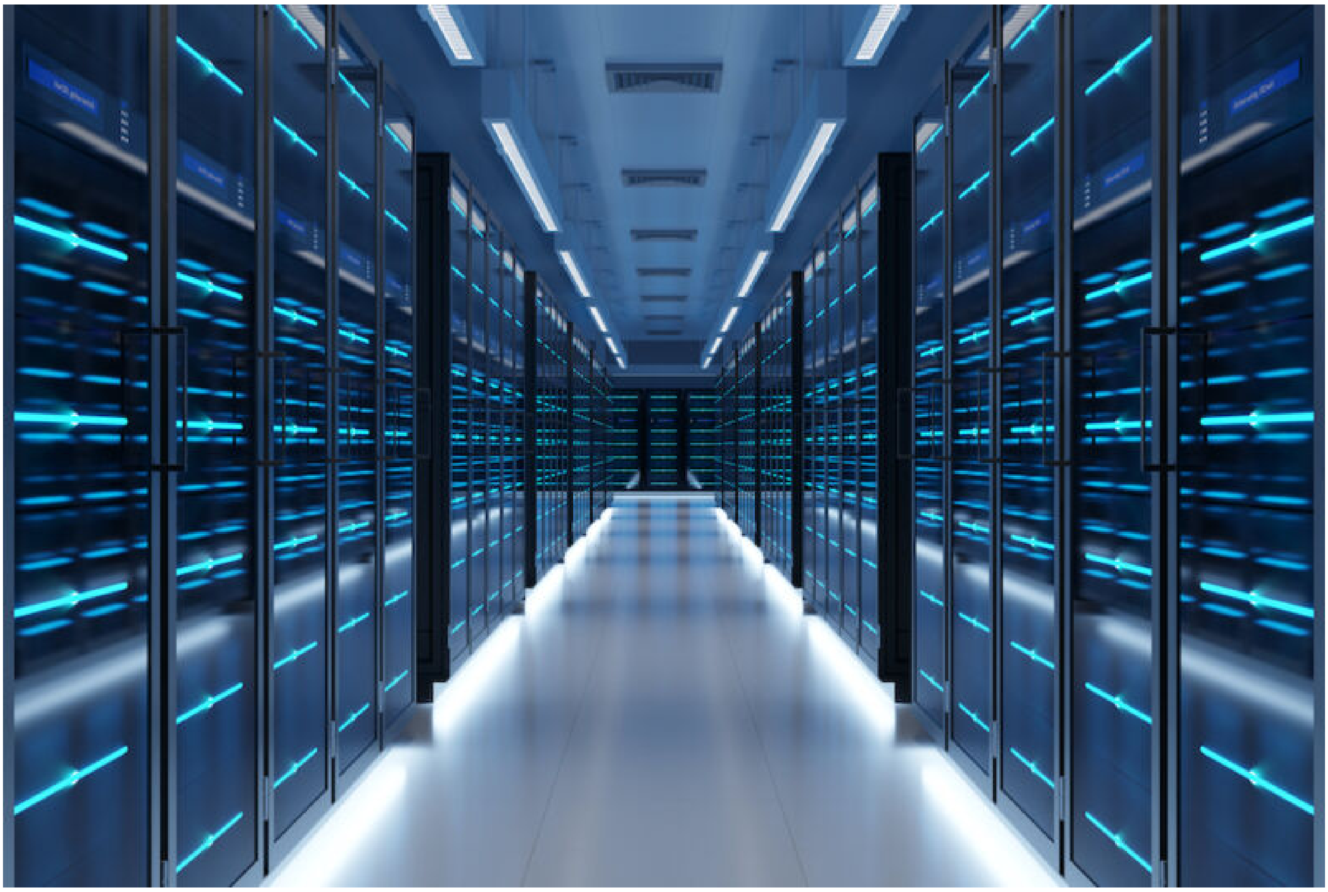
Omnipotent BMCs from Quanta remain vulnerable to critical Pantsdown threat



Getty Images

reader comments

46 with 42 posters participating

Share this story

In January 2019, a researcher disclosed a devastating vulnerability in one of the most powerful and sensitive devices embedded into modern servers and workstations. With a severity rating of 9.8 out of 10, the vulnerability affected a wide range of baseboard management controllers (BMC) made by multiple manufacturers. These tiny computers soldered into the motherboard of servers allow cloud centers, and sometimes their customers, to streamline the remote management of vast fleets of computers. They enable administrators to remotely reinstall OSes, install and uninstall apps, and control just about every other aspect of the system—even when it’s turned off.

Pantsdown, as the researcher dubbed the threat, allowed anyone who already had some access to the server an extraordinary opportunity. Exploiting the arbitrary read/write flaw, the hacker could become a super admin who persistently had the highest level of control for an entire data center.

The industry mobilizes… except for one

Over the next few months, multiple BMC vendors issued patches and advisories that told customers why patching the vulnerability was critical.

Now, researchers from security firm Eclypsium reported a disturbing finding: for reasons that remain unanswered, a widely used BMC from data center solutions provider Quanta Cloud Technology, better known as QCT, remained unpatched against the vulnerability as recently as last month.

As if QCT’s inaction wasn’t enough, the company’s current posture also remains baffling. After Eclypsium privately reported its findings to QCT, the solutions company responded that it had finally fixed the vulnerability. But rather than publish an advisory and make a patch public—as just about every company does when fixing a critical vulnerability—it told Eclypsium it was providing updates privately on a customer-by-customer basis. As this post was about to go live, “CVE-2019-6260,” the industry’s designation to track the vulnerability, didn’t appear on QCT’s website.

In an email, Eclypsium VP of Technology John Loucaides wrote:

> *Eclypsium is continuing to find that custom servers (eg. Quanta) remain unpatched to vulnerabilities from as far back as 2019. This is affecting a myriad of devices from a large number of cloud providers. The problem isn’t any one vulnerability, it’s the system that keeps cloud servers old and vulnerable. Quanta has only just released the patch for these systems, and they did not provide it for verification. In fact, their response to us was that it would only be made available upon request to support.”*

Multiple Quanta representatives didn’t respond to two emails sent over consecutive days requesting confirmation of Eclypsium’s timeline and an explanation of its patching process and policies.

Current, but not patched

A blog post Eclypsium published on Thursday shows the type of attack that’s possible to carry out on QCT BMCs using firmware available on QCT’s update page as of last month, more than three years after Pantsdown came to light.

Eclypsium’s accompanying video shows an attacker gaining access to the BMC after exploiting the vulnerability to modify its web server. The attacker then executes a publicly available tool that uses Pantsdown to read and write to the BMC firmware. The tool allows the attacker to supply the BMC with code that opens a reverse web shell whenever a legitimate administrator refreshes a webpage or connects to the server. The next time the admin tries to take either action, it will fail with a connection error.

Behind the scenes, however, and unbeknownst to the admin, the attacker’s reverse shell opens. From here on, the attacker has full control of the BMC and can do anything with it that a legitimate admin can, including establishing continued access or even permanently bricking the server.

[embedded content]
BMC Attack Demo
The power and ease of use of the Pantsdown exploit are by no means new. What is new, contrary to expectations, is that these types of attacks have remained possible on BMCs that were using firmware QCT provided as recently as last month.

QCT’s decision not to publish a patched version of its firmware or even an advisory, coupled with the radio silence with reporters asking legitimate questions, should be a red flag. Data centers or data center customers working with this company’s BMCs should verify their firmware’s integrity or contact QCT’s support team for more information.

Even when BMCs come from other manufacturers, cloud centers, and cloud center customers shouldn’t assume they’re patched against Pantsdown.

“This is a serious problem, and we do not believe it is a unique occurrence,” Loucaides wrote. “We’ve seen currently deployed devices from each OEM that remain vulnerable. Most of those have updates that simply were not installed. Quanta’s systems and their response did set them apart, though.”

https://arstechnica.com/?p=1856683