Security team discussed weakness in bare-metal services

February 27 2019, by Nancy Cohen

Credit: CC0 Public Domain

Back door open. Never a good sign in a computer security environment. Researchers poking around are sure to call out their discoveries in an instance such as the recent one, where cloud servers looked as if they could be compromised.

Beaverton, Oregon-based security watchers Eclypsium had been exploring how malware could be injected into bare metal cloud servers. The feat was a BMC hack.

What are BMCs? Dan Goodin in *Ars Technica* said these are "motherboard-attached microcontrollers that give extraordinary control over servers inside datacenters."

BMC stands for Baseboard Management Controller. Here is IBM's definition. "The Baseboard Management Controller (BMC) is a third-party component designed to enable remote management of a server for initial provisioning, operating system reinstall and troubleshooting. As part of IBM Cloud's Bare Metal Server offering, clients have access to the BMC."

Alex Bazhaniuk on the Eclypsium site had warned of possible BMC issues before Eclypsium's most recent report. Back in August, he pointed out that "the BMC has become a particularly hot area of investigation for security researchers."

While BMCs might serve a critical need for data centers, they also present a risk.

As Goodin found, warnings over BMCs and possible security weaknesses could be traced back further, as In 2013, when researchers warned that BMCs preinstalled in servers from some big name-brand manufacturers were poorly secured. In turn, attackers could possibly have "a stealthy and convenient way to take over entire fleets of servers inside datacenters."

In the latest findings, the researchers delivered a detailed blog that examined security implications for bare-metal and general cloud services. That blog also included best-practice advice for cloud service customers and service providers.

In a "bare metal" cloud model, BMC vulnerabilities can undermine this model by allowing a customer to leave a backdoor that will remain active once the server is reassigned, said Goodin.

On that same note, *BleepingComputer*'s Sergiu Gatlan wrote that "bare metal servers can be compromised by potential attackers which could add malicious backdoors and code in the firmware of a server or in its baseboard management controller (BMC) with minimal skills."

So, these "client reassignments" are where problems can show up.

In *BleepingComputer*, Gatlan summed up the Eclypsium discovery, where "attackers can implant malicious backdoors within the firmware of cloud services' shared infrastructure, with these implants being able to survive after the cloud service provider distributes the server to another customer."

He said the vulnerability allows attackers to implant backdoor implants in the firmware or BMC of bare metal servers that survive client reassignment in bare metal and general cloud services.

With the customer open to attacks, the scenarios can range from data theft, to denial of service, to ransomware.

When security hounds bark, meanwhile, IBM listens. And if the barks merit not only attention but action, then they respond. On Monday, IBM said it recognized the vulnerability. "On some system models offered by IBM Cloud and other cloud providers," said the blog post, "a malicious attacker with access to the provisioned system could overwrite the firmware of the BMC." The system could be returned to the hardware pool. The compromised BMC firmware could be used to attack the next user of the system.

One could not help but notice that IBM described the issue as "low severity." After all, "The BMC has limited processing power and memory, which makes these types of attacks difficult," said IBM. Moreover, the company said they did not find any indication of an exploit via this vulnerability for malicious purposes.

What, then, action was IBM proposing?

"IBM has responded to this vulnerability by forcing all BMCs, including those that are already reporting up-to-date firmware, to be reflashed with factory firmware before they are re-provisioned to other customers. All logs in the BMC firmware are erased and all passwords to the BMC firmware are regenerated."

Computer Business Review: "Bare metal refers to an exclusively leased server in a cloud data centre, rather than Infrastructure-as-a-Service (IaaS) involving VMs that use physical servers for multiple cloud clients."

As Eclypsium noted, most standard IaaS service options will have multiple customers share the resources of an underlying physical server and some customers will have high performance requirements for their applications or possess sensitive data that they don't want to have stored on a shared machine.

"For these high-value applications, cloud service providers offer bare-metal cloud options in which customers buy access to dedicated, physical servers they can use in any way they see fit. There is no need to worry about buying and supporting hardware—they can grow on-demand as needed."

As with all cloud services, once a customer is done using a bare-metal server, the hardware is reclaimed by the service provider and repurposed for another customer.

Gatlan's parting advice: "While bare metal cloud offerings are very convenient for organizations which do not want to invest in their own hardware, security concerns such as the one the Eclypsium research team unearthed might convince them to switch to hardware that they own and manage on-site to avoid having sensitive data accessed or modified, as well as critical apps disabled."

More information: eclypsium.com/2019/01/26/the-m … etal-cloud-services/

Citation: Security team discussed weakness in bare-metal services (2019, February 27) retrieved 10 April 2024 from https://techxplore.com/news/2019-02-team-discussed-weakness-bare-metal.html