The BMC and IPMI Vulnerabilities

EMERSON
Network Power

The BMC and IPMI Vulnerabilities

Table of Contents

Executive Summary

Potential security flaws in the Baseboard Management Controllers (BMCs), also known as service processors, and the Intelligent Platform Management Interface (IPMI) protocol have been exposed by recent analyst studies[1,4]. The Avocent solutions effectively address these security vulnerabilities related to the BMCs and IPMI with its latest Avocent MergePoint™ Embedded Management Software and OEM offerings.

Recently some IT security analysts have published reports detailing some potential vulnerabilities with IPMI and how they are sometimes exploited. Many follow-up articles within the IT community have been published including the US Government (TA13-207A). All the new security-related attention has prompted action by most server vendors to patch their service processor weaknesses. Some of the vulnerabilities are present only in older generation servers and have been resolved in newer server implementations, as expected. Many of the worst vulnerabilities discovered in the reports are attributed to IPMI implementations produced by smaller vendors with limited expertise. A common thinking in the industry is that Avocent/Emerson has been the leading provider for IPMI firmware to major server vendors for years. However, the fact is that not all server models/generations from those vendors were developed in partnership with the Avocent solution.

Many of the flaws highlighted recently are based on misconfiguration of IPMI-compatible BMCs tested in the surveys. These misconfigurations occur due to a lack of awareness and/or poorly designed firmware for the BMCs. As a result, data centers maintained within standard practices and that use the BMCs from leading vendors are not susceptible to these threats. This, of course, is in addition to regular server maintenance including patching, proper configuration and password-encryption procedures.

The Avocent solutions recommend the use of out-of-band (OOB) management networks, which are independent of the corporate network, to efficiently access servers for triage, configuration and troubleshooting via the BMC. OOB management networks are IP networks that are either physically separated or separated with VLANs from the main production network. The lynchpin in typical setups is the compromise between security, usability and accessibility. Such compromises often create a solution that does not satisfy all user needs while still jeopardizing security. Alternative and customized solutions could, at best, incorporate some best practices and incorporate “jump boxes” or dual-homed systems in order to provide some secure access to the OOB management LANs. The most complete, and best, out-of-band access platform solution incorporates the Avocent® Universal Management Gateway appliance which is a secure gatekeeper that provides access between users and thousands of BMCs on the OOB management LAN. The Avocent solution provides full, real-time access to the service processor/BMC through a simple and secure UI while completely protecting access to the data center OOB management LAN.

The Open Doors

A BMC is a specialized microcontroller embedded in most server platforms. It interfaces with the CPU, fans, power supplies and a myriad of sensors to facilitate monitoring and KVM, media and power control of the managed server or "host". The BMC is functionally independent from the host operating system despite tight coupling with the server hardware. The BMC is online and functional as long as the server is plugged into a power source. The server does not need to be powered up (with fans spinning) for the BMC to provide remote management to the server.

Here lies the problem: the BMC's core strength (the ability to fully configure, control, triage and administer a server) can be cause for concern with IT operations and the network security professionals due to its potential for misuse.

This is because the BMC is an autonomous compute node that functions independently of the operating system providing a secondary form of access to the server. The BMC is a "black box" operating in tandem with the host hardware and unfamiliar to all but the select few professionals working in the server industry. For some security research professionals, the idea of a secondary access path into the server ecosystem which is poorly understood is terrifying and warrants industry attention, proper design and auditable oversight.

Can the BMC be exploited? Potentially, and those with poorly developed firmware are particularly vulnerable. A delicate balance must be struck between preserving the BMCs' usefulness to the operator and securing the BMC access. This necessitates both solid firmware development by vendors and best practices by data center operators to be sure the BMCs are well-managed. A prime example is ensuring the BMC uses authorization protocols, non-default and non-shared authentication credentials and the BMC LAN interface is on a closed/protected network or VLAN integrated with secure access gateways.

On IPMI

IPMI is an IP-based UDP protocol standard that has been widely adopted by most server manufacturers and the open-source community. IPMI provides a standardized communication paradigm among disparate vendor hardware products. Think of it as the communication conduit that enables server hardware to be remotely controlled and accessed by users and software from anywhere in the world.

The IPMI standard is controlled by an Intel-sponsored working group which has over 200 adopters since version 1.0. It is the most widely deployed standard for interaction with the server BMCs. Further development to the standard is still ongoing through derivatives such as Data Center Management Interface (DCMI).

The latest version of the protocol is IPMI 2.0, revision 5 (2009). IPMI 2.0 addresses security vulnerabilities identified in the previous 1.5 revision. This includes specifying RMCP+ for authentication, encryption and role-based user configuration on the IPMI over LAN interface.

The Holes

A DARPA study, highlighted in recent publications, has revealed that despite these enhancements, IPMI 2.0 exposes several security vulnerabilities[1,2]. There are six major factors listed in the study related to IPMI and certain BMC solutions:

1. **IPMI Cipher Suite 0:** Configuring the IPMI stack for cipher suite ID 0 support allows authentication-less IPMI session access to the BMC with Administrator level privileges- if so configured.
2. **Anonymous Login:** IPMI allows configuration of "NULL" valued username and password settings for anonymous login without username or password.
3. **BMC Universal Plug and Play (UPnP) Support:** Some BMC/BMC solutions support Universal Plug and Play by default. UPnP is meant to simplify interconnecting networked devices, but it is prone to exposing the host to multiple security exploits[3].
4. **IPMI Password Stored in Clear-Text:** Certain BMC solutions may store user IPMI passwords in clear-text on the BMC non-volatile memory. This is a security vulnerability potentially compromising the whole data center in the event that even a single BMC is exploited where common/shared credentials are used. Reliance on default or common/shared authentication credentials is a poor practice and should be avoided by every administrator.
5. **Get Channel Authentication Capabilities Command:** This IPMI command is used to obtain authentication capabilities from the target BMC including anonymous login and NULL username enabled. This is only considered a flaw, which could weaken BMC security by exposing other vulnerabilities listed in the study.
6. **RAKP Hashed Password:** IPMI RMCP+ uses the Remote Authenticated Key-Exchange Protocol (RAKP). This protocol sends a cryptographic hash of the user password to the remote client during authentication. The hashed password can be subject to offline brute-force attacks compromising the password.

Avocent Response

The Avocent solutions provide robust secure management solutions to its customers. The Avocent BMC/BMC firmware effectively addresses/mitigates the key security concerns raised around IPMI and the BMC, such as the first four security issues:

1. Avocent firmware disables IPMI Cipher Suite 0 by default.
2. Avocent firmware disables IPMI anonymous login by default and does not support "NULL" passwords.
3. Avocent firmware does not support UPnP.
4. Avocent firmware does not support clear-text password storage. All passwords stored in non-volatile memory are encrypted.

The *Get Channel Authentication Capabilities* command (5) is not truly a vulnerability. The command is required by the IPMI protocol and is supported by the Avocent firmware. However, the Avocent firmware does not support anonymous login for this command, eliminating the security impact.

Authentication with RAKP (6) requires hashing and transmitting the user password to the remote client in order to authenticate with vendor-specific remote management tools. The study recommends using long and complex passwords to mitigate this vulnerability. This falls squarely on the shoulders of password policy best practices and maintaining a secure and private OOB management network, as discussed earlier.

Containing the Risk – OOB Networks

The majority of the BMCs offer direct or shared configuration options for network connections. Shared "side-band" connections provide the BMC access via the server system network interface on the production network using separate MAC and IP addresses. Direct connected BMC deployments utilize a dedicated Ethernet port and are physically connected to either a production or private management network. We can summarize the BMC network paradigms as:

- Logically connected and logically managed: The simple side-band deployment type that is logically connected and logically managed since it is both physically connected to a production network and is IP-accessible from the production network.
- Physically connected and logically managed: Direct connected BMC on a production network.
- Physically connected and physically managed: Direct connected BMC on a private management network.

The benefits of logical connections are cabling convenience and cost savings. The benefit of logical management is simplicity and "ease of access" for users/operators. The risks to logical connections and logical management are security and auditability. It is possible for servers to be secured when their BMCs are logically connected and logically managed but only if they are free from vulnerabilities and have properly maintained passwords. This type of convenience and security comes at the cost of significant administrative overhead. Minimizing the overhead and security risks can be easily achieved when the BMCs are securely deployed instead.

Secure deployment models are recommended by industry analysts, security experts and even the US Computer Emergency Readiness Team (US-CERT). For example: The US-CERT TA13-207A recommends that administrators should restrict IPMI traffic to trusted internal networks and monitor all user access to and within that network.

The BMC and IPMI Vulnerabilities

To achieve secure BMC deployment, many experienced network engineers implement private networks for isolating the BMCs and other low-level management interfaces/consoles. Private networks are largely inaccessible to outside networks containing users. A simple example would have an isolated set of network switches which host a non-production IP subnet that is only accessible through a dual-homed system called a "jump box". Private networks inherently increase security by preventing detection of the BMCs due to malicious IP scanning. Server administrators who are authorized to access the BMCs can do so remotely through the jump box. A modern alternative to the jump box and isolated switches is a firewall and a private VLAN with a secure VPN to provide remote administrator access. This type of custom solution will be effective at the BMC deployment security with minimal feature compromise. However, this custom solution can be complex to set up and difficult to maintain for a moderate- and large-sized user base.

The best solution is to leverage a purpose-built solution such as the Avocent® Universal Management Gateway appliance. This appliance combines the best functionalities of a jump box and a firewall into a simple solution for the BMC security without compromise of convenience. This solution supports convenient side-band logical BMC connections to an isolated VLAN and also provides a physical separation of the management data behind strong authentication, authorization and accounting mechanisms for user access.

Logical Connection and Physical Management

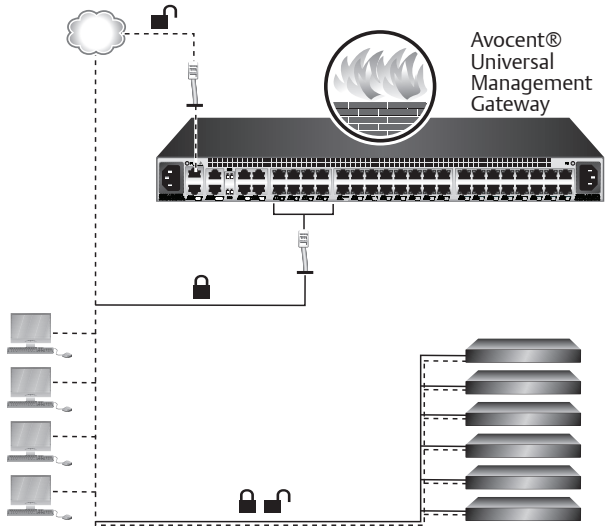

Figure 1: Example of a Secure Management Network for BMCs, which are only logically separated from the production LAN with VLAN tags. User access is physically separated and safely provided through the Avocent® Universal Management Gateway appliance.

The preceding solutions provide a strong "front-door" approach to securing the BMCs within an isolated network. These solutions do not protect other BMCs within the isolated network from attack by authenticated access to a different BMC. Put another way, these solutions are effective at corralling any IPMI vulnerabilities into an area that warrants high scrutiny of user access which, when implemented correctly, will significantly diminish the BMC security risks. For many companies/industries, this should be enough. However, there is an increased interest in security within the greater IT industry that warrants administrators taking a closer look at how to connect and secure the BMCs within their private networks.

The risk within the private network stems for granting legitimate access for one user to one specific system and that user maliciously exploiting a vulnerable BMC to attack the other BMCs on the network. The only way to prevent such violations is to isolate all BMCs from each other. This style of isolation can only be implemented with physically connected BMCs. The switch providing the physical connections must be configured to isolate each BMC into its own private VLAN. This implementation requires heavily configured firewalls and private VLAN switches that are vigilantly maintained or vendor-supplied and purpose-built technologies. An additional consideration is the risk of human error in the configuration and maintenance of the general-purpose network hardware implementing the solution vs. preconfigured solutions that are designed and tested to provide a hardened level of security and support.

The Avocent® Universal Management Gateway appliance is a purpose-built appliance that mitigates the risks associated with the BMC deployments and simplifies the processes for providing users with access. The Avocent® Universal Management Gateway appliance has 40 isolated and private ethernet ports that can be used for physically connecting and securing BMCs. These private ports, each one secure from the next, will not allow a malicious user with access to one BMC to exploit a feature/vulnerability in that BMC and attack any of the other BMCs protected by the Avocent® Universal Management Gateway appliance.

The Avocent® Universal Management Gateway appliance implements user permissions for the BMC features allowing it to function as a trustworthy liaison between the actions of a user and the capabilities of a BMC (i.e. power on/off, sensors, event logs) without admitting the user to directly interact with the BMC. When it becomes necessary for the user to launch remote console sessions through the BMC (i.e Serial over LAN, vKVM, vMedia, SSH, Browser sessions), the appliance will create secure proxy tunnels to connect the user with the BMC quickly and conveniently. The Avocent® Universal Management Gateway appliance simplifies the BMC management while also preventing exploitation by removing the risks of IPMI vulnerabilities and "out of sight, out of mind" human mistakes.

Physical Connection and Physical Management

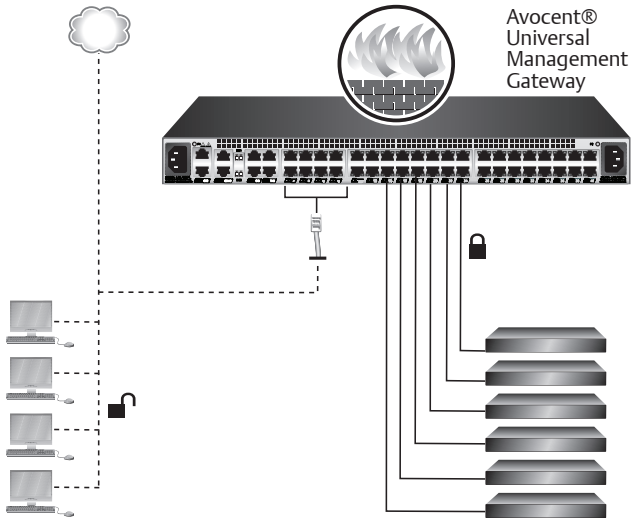

Figure 2: Example of most secure deployment style for BMCs, which are physically separated from the production LAN with dedicated connections. User access is physically separated and safely provided by the Avocent® Universal Management Gateway appliance.

Sources

[1]Rapid7. (2013). Widespread Vulnerabilities in Baseboard Management Controllers (BMCs) and the Intelligent Platform Management Interface (IPMI) Frequently Asked Questions [White paper]. Retrieved from https://community.rapid7.com/servlet/JiveServlet/download/2344-1-22100/Widespread%20Vulnerabilities%20in%20Baseboard%20Management%20Controllers%20-%20FAQ%20.pdf

[2]Zetter, Kim. (2013). Hacker Holes in Server Management System Allow 'Almost-Physical' Access. Retrieved July 02, 2013, from http://www.wired.com/threatlevel/2013/07/ipmi/

[3]Rapid7. (2013). Security Flaws in Universal Plug and Play

Unplug. Don't Play [White paper]. Retrieved from https://community.rapid7.com/servlet/JiveServlet/download/2150-1-16596/SecurityFlawsUPnP.pdf

[4] Farmer, Dan. (2013). IPMI: FREIGHT TRAIN TO HELL [White paper]. Retrieved from http://fish2.com/ipmi/

[5] Mimoso, Michael (2013). IPMI Protocol, BMC vulnerabilities Expose Thousands of Servers to Attack http://threatpost.com/ipmi-protocol-bmc-vulnerabilities-expose-thousands-of-servers-to-attack

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), delivers software, hardware and services that maximize availability, capacity and efficiency for data centers, health care and industrial facilities. A trusted industry leader in smart infrastructure technologies, Emerson Network Power provides innovative data center infrastructure management solutions that bridge the gap between IT and facility management and deliver efficiency and uncompromised availability regardless of capacity demands. Our solutions are supported globally by local Emerson Network Power service technicians. Learn more about Emerson Network Power products and services at **www.EmersonNetworkPower.com.**

Emerson Network Power
EmersonNetworkPower.com

1013-BMC_IPMI_VULNERABILITIES-WP-EN