VIRTUAL MEDIA VULNERABILITY IN BMC OPENS SERVERS TO REMOTE ATTACK

Most security professionals are appropriately wary of unknown USB devices, and would (hopefully) never pick up an unknown, untrusted USB drive and plug it into their computer. However, our research has uncovered new vulnerabilities, which we collectively dubbed USBAnywhere, in the baseboard management controllers (BMCs) of Supermicro servers, which can ***allow an attacker to easily connect to a server and virtually mount any USB device of their choosing to the server, remotely over any network including the Internet***. At the time of writing, we found at least 47,000 systems with their BMCs exposed to the Internet and using the relevant protocol. It is important to remember that these are only the BMCs that are directly exposed to the Internet. The same issues can be easily exploited by attackers who gain access to a corporate network.

Security researchers and others interested in the technical details of the vulnerabilities will want to visit our GitHub repository at https://github.com/eclypsium/USBAnywhere.

INTRODUCTION

By design, BMCs are intended to allow administrators to perform out-of-band management of a server, and as a result are highly privileged components. In this case, the problem stems from several issues in the way that BMCs on Supermicro X9, X10 and X11 platforms implement virtual media, an ability to remotely connect a disk image as a virtual USB CD-ROM or floppy drive. When accessed remotely, the virtual media service allows plaintext authentication, sends most traffic unencrypted, uses a weak encryption algorithm for the rest, and is susceptible to an authentication bypass. These issues allow an attacker to easily gain access to a server, either by capturing a legitimate user's authentication packet, using default credentials, and in some cases, without any credentials at all.

Once connected, the virtual media service allows the attacker to interact with the host system as a raw USB device. This means attackers can attack the server in the same way as if they had physical access to a USB port, such as loading a new operating system image or using a keyboard and mouse to modify the server, implant malware, or even disable the device entirely. The combination of easy access and straightforward attack avenues can allow unsophisticated attackers to remotely attack some of an organization's most valuable assets.

GAINING REMOTE USB ACCESS

Normally, access to the virtual media service is facilitated by a small Java application served by the BMC's web interface. This application then connects to the virtual media service listening on TCP port 623 on the BMC. The service uses a custom packet-based format to authenticate the client and transport USB packets between client and server.

Our analysis of the authentication revealed the following issues:

- **Plaintext Authentication**
  While the Java application uses a unique session ID for authentication, the service also allows the client to use a plaintext username and password.

- **Unencrypted network traffic**
  Encryption is available but must be requested by the client. The Java application provided with the affected systems use this encryption for the initial authentication packet but then use unencrypted packets for all other traffic.

- **Weak encryption**
  When encryption is used, the payload is encrypted with RC4 using a fixed key compiled into the BMC firmware. This key is shared across all Supermicro BMCs. RC4 has multiple published cryptographic weaknesses and has been prohibited from use in TLS (RFC7465).

- **Authentication Bypass** (X10 and X11 platforms only)
  After a client has properly authenticated to the virtual media service and then disconnected, some of the service's internal state about that client is incorrectly left intact. As the internal state is linked to the client's socket file descriptor number, a new client that happens to be assigned the same socket file descriptor number by the BMC's OS inherits this internal state. In practice, this allows the new client to inherit the previous client's authorization even when the new client attempts to authenticate with incorrect credentials.

Taken together, these weaknesses open several scenarios for an attacker to gain unauthorized access to virtual media. In the simplest case, an attacker could simply try the well-known default username and password for the BMC. However, even if the default password was changed, an attacker could still easily gain access. If a valid administrator had used virtual media since the BMC was last powered off, the authentication bypass vulnerability would allow an attacker to connect even without the proper username and password. Given that BMCs are intended to be always available, it is particularly rare for a BMC to be powered off or reset. As a result, the authentication bypass vulnerability is likely to be applicable unless the server has been physically unplugged or the building loses power.

Alternatively, the attacker could intercept traffic to the virtual media service and decrypt it with the fixed key stored both on the BMC and in the Java application. This last example would, of course, require the attacker to be in a position to intercept traffic.

A scan of TCP port 623 across the Internet revealed 47,339 BMCs from over 90 different countries with the affected virtual media service publicly accessible.

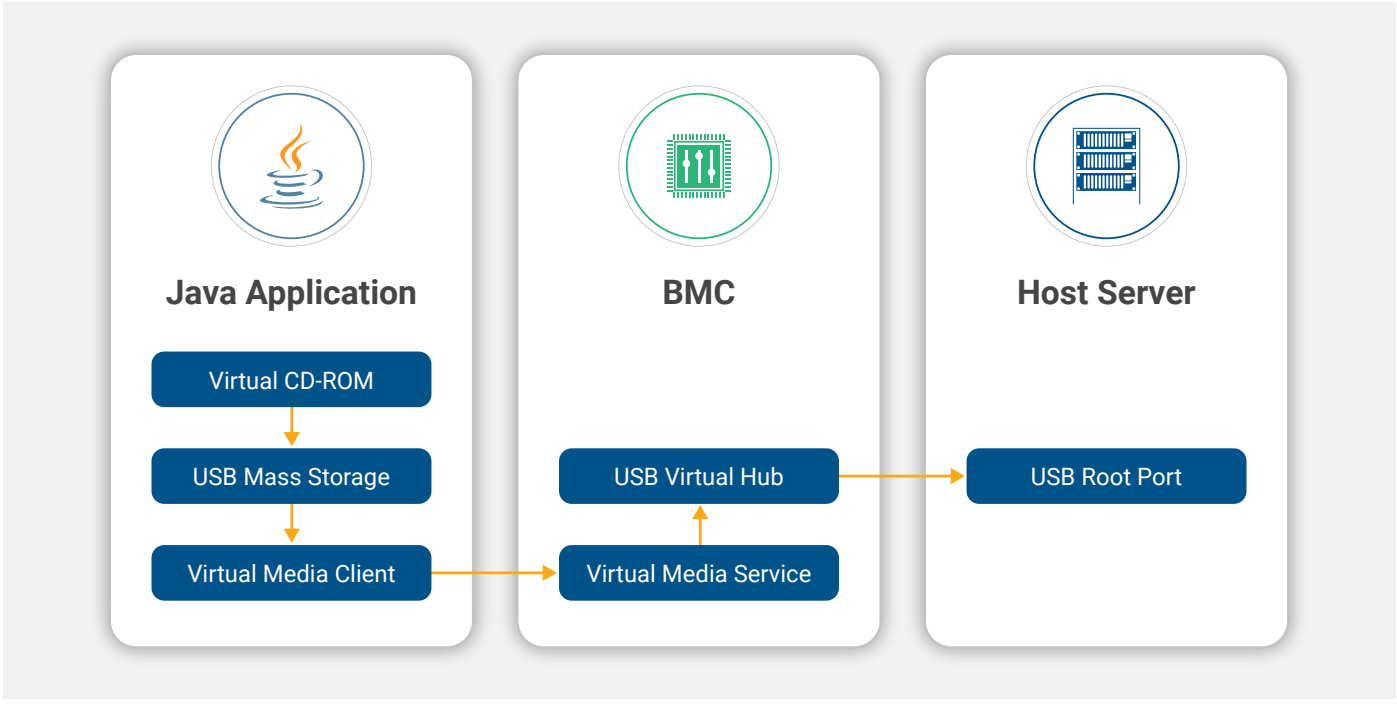
RAW USB ACCESS TO HOST SYSTEM

Once authenticated, the user can access a virtual USB hub on the BMC. This virtual hub supports up to 5 virtual downstream devices that can be configured in almost any fashion.

Normally, when a new USB is attached to a host, the new device presents the host with "descriptors" to identify the type of device and its configuration. For example, these descriptors are how a system can distinguish between a USB CD-ROM drive versus a printer versus a WiFi adapter and load the corresponding device drivers. The user is then able to interact with the host system by sending and receiving data over the USB endpoints defined by those descriptors.

However, the devices within the virtual USB hub of the Supermicro devices rely on software on the BMC to provide these descriptors. ***Consequently, the BMC hardware allows the software to be any USB device***. This is how the Java application can be a virtual CD-ROM drive.

When coupled with frameworks such as Facedancer, which allow users to implement USB devices in software, an attacker can emulate any device they need. Such a combination of functionality could allow an attacker to boot the machine from a malicious USB image, exfiltrate data over a USB mass storage device, or use a virtual USB Rubber Ducky that rapidly performs a sequence of carefully crafted keystrokes to perform virtually any other type of hacking against the BMC, the firmware, or the server it manages. In this video, our researchers demonstrate a proof-of-concept data exfiltration attack using Facedancer.



BEST PRACTICES FOR SECURING BMCS

It is important to note that BMCs should never be directly exposed to the Internet. While the underlying issues described here would apply to connections over any network, direct exposure to the Internet greatly increases the likelihood of an attack.

BMCs are some of the most privileged components in enterprise technology today. With the ability to provide remote, out-of-band management for servers, BMCs provide virtually omnipotent control over a server and its contents. BMCs have also become one of the most active areas of security research due to their importance and reputation for being riddled with vulnerabilities. While it is well-known security best practice to isolate BMCs on their own private and secured network segment, it is also well-known that many organizations forget or ignore this step. A simple SHODAN scan reveals that there are at least 92,000 BMCs that are easily discoverable on the Internet at the time of this writing.

Given the speed with which new BMC vulnerabilities are being discovered and their incredible potential impact, there is no reason for enterprises to risk exposing them directly to the Internet.

BMCs that are not exposed to the Internet should also be carefully monitored for vulnerabilities and threats. While organizations are often fastidious at applying patches for their software and operating systems, the same is often not true for the firmware in their servers.

Furthermore, this research should serve as a stark reminder that some BMC vulnerabilities can be easily abused even by unsophisticated attackers. While historically firmware attacks required either physical presence or an initial compromise of the OS, modern firmware and remote management functionality has increased the attack surface to include remote attacks directly against firmware. In this case, attackers with little more than a free tool to emulate a USB device can remotely gain full control over an enterprise server. Just as applying application and OS security updates has become a critical part of maintaining IT infrastructure, keeping abreast of firmware security updates and deploying them regularly is required to defend against casual attacks targeting system firmware.

MITIGATION

Supermicro quickly responded to disclosures from Eclypsium and collaborated with the Eclypsium team to develop a fix for the vulnerabilities described herein. Supermicro has committed to providing firmware updates for their X9, X10 and X11 platforms. Organizations using the Supermicro X9, X10 and X11 platforms are encouraged to visit Supermicro's Security Center and Virtual Media Vulnerability details page for information on updating BMC firmware on these platforms.

In addition to vendor-supplied updates, organizations should adopt tools to proactively ensure the integrity of their firmware and identify vulnerabilities, missing protections, and any malicious implants in their firmware.

SUMMARY

Through these vulnerabilities, an attacker can bypass authentication to access virtual media or, alternatively, intercept virtual media traffic to recover BMC credentials and capture data sent over virtual media devices. Further, the affected systems are shipped with default BMC credentials that have been found to be frequently unchanged, even on Internet-connected BMCs. Once credentials are obtained, an attacker can then perform any of a large number of USB-based attacks against the server remotely including data exfiltration, booting from untrusted OS images, or direct manipulation of the system via a virtual keyboard and mouse.

This vulnerability further highlights the importance of monitoring and securing servers beyond the scope of the operating system and applications they run. Servers have an exceedingly broad firmware attack surface, of which BMCs are but one example. Network adapters, physical ports, drives, processors and chipsets, and dozens of other components rely on firmware that contain exploitable vulnerabilities. Threats operating at this level can easily subvert traditional security measures and put the device, the system it is part of, and the integrity of all data stored on that system at risk. Monitoring firmware integrity and deploying firmware security updates are fundamental measures to build solid server security.

DISCLOSURE TIMELINE

2019-06-19:	Eclypsium reports vulnerability to Supermicro
2019-07-09:	Eclypsium reports additional findings to Supermicro
2019-07-29:	Supermicro acknowledges report and develops a fix
2019-08-16:	Eclypsium notifies CERT/CC due to large number of public systems affected
2019-08-16:	Supermicro confirms intent to publicly release firmware by September 3rd
2019-08-21:	Eclypsium attempts to notify CERT/CC for the second time
2019-08-23:	Eclypsium notifies network operators whose networks contain affected, Internet-accessible BMCs
2019-08-23:	Eclypsium discovers that Supermicro X9 platforms are also affected
2019-09-03:	Eclypsium publishes vulnerability details and presents same at Open Source Firmware Conference