Los servidores empresariales que funcionan con placas Supermicro, pueden resultar comprometidos de forma remota al conectar virtualmente dispositivos USB maliciosos, según informaron investigadores de seguridad cibernética de Eclypsium.

En este caso, es posible lanzar todo tipo de ataques USB contra servidores vulnerables de Supermicro sin acceder de forma física a ellos o esperar a que la víctima recoja una unidad USB desconocida.

Apodado como *«USBAnywhere»*, el ataque aprovecha distintas vulnerabilidades recientemente descubiertas en el firmware de los controladores BMC que podrían permitir que un atacante remoto no autorizado se conecta a un servidor Supermicro y monte virtualmente un dispositivo USB malicioso.

Con la mayoría de los conjuntos de chips de servidor, viene integrado un controlador de administración de placa base (BMC), que es un chip de hardware en el núcleo de las utilidades de la interfaz de administración de plataforma inteligente (IPMI) que permite a los administradores de sistema controlar y monitorear remotamente un servidor sin tener que acceder al sistema operativo o aplicaciones que se ejecuten en él.

De este modo, BMC es un sistema de administración fuera de banda que permite a los administradores reiniciar remotamente un dispositivo, analizar registros, instalar un sistema operativo y actualizar el firmware, lo que lo convierte en uno de los componentes más privilegiados en la tecnología empresarial actual.

Una de esas capacidades de BMC incluye el montaje de medios virtuales para conectar una imagen de disco como un CD-ROM, USB Virtual o unidad de disquete con un servidor remoto.

Según un informe publicado hoy por Eclypsium, los BMC en las plataformas Supermicro X9, X10 y X11 utilizan una implementación insegura para autenticar al cliente y transportar paquetes USB entre el cliente y el servidor.

Estas debilidades pueden ser explotadas fácilmente por un hacker remoto para evitar el

proceso de autenticación por medio del servicio de medios virtuales que escucha el puerto TCP 623 o interceptar el tráfico para recuperar credenciales de BMC débilmente encriptadas o credenciales sin encriptar.

Dichas debilidades incluyen:

- Autenticación en texto plano
- Tráfico de red sin encriptar
- Cifrado débil
- Bypass de autenticación (solo plataformas X10 y X11)

> *«Cuando se accede remotamente, el servicio de medios virtuales permite la autenticación de texto sin formato, envía la mayor parte del tráfico sin cifrar, utiliza un algoritmo de cifrado débil para el resto y es susceptible a una omisión de autenticación. Estos problemas permiten que un hacker obtenga fácilmente acceso a un servidor, ya sea capturando el paquete de autenticación de un usuario legítimo, utilizando credenciales predeterminadas y, en algunos casos, sin ninguna credencial»,* dijeron los investigadores.

Una vez conectado, el servicio de medios digitales comprometido permite a los atacantes interactuar con el sistema host como un dispositivo USB sin procesar, lo que les permite realizar todo lo que se puede hacer con acceso físico a un puerto USB, incluyendo:

- Exfiltración de datos
- Implante de malware
- Arranque desde imágenes de sistema operativo no confiables
- Manipulación directa del sistema a través de un teclado y mouse virtuales
- Deshabilitar el dispositivo por completo

Según los investigadores, un escaneo del puerto TCP 623 por medio de Internet, reveló más de 47 mil BMC de más de 90 países diferentes con el servicio de medios virtuales de

firmware BMC afectado.

Además de explotar los BMC donde los servicios de medios virtuales están expuestos directamente en Internet, estos defectos también pueden ser explotados por un atacante con acceso a una red corporativa cerrada o atacantes intermedios dentro de las redes del lado del cliente.

Los investigadores informaron sus hallazgos a Supermicro en junio y julio de este año. La compañía reconoció los problemas en agosto y lanzó públicamente una actualización de firmware para sus plataformas X9, X10 y X11 antes del 3 de septiembre.

Por lo tanto, las organizaciones deberían actualizar su firmware BMC lo antes posible. Además, es importante asegurarse de que los BMC nunca se expongan directamente a Internet, ya que la exposición directa a Internet aumenta en gran medida la probabilidad de dichos ataques.