Se revelaron tres vulnerabilidades de seguridad diferentes en el software MegaRAC Baseboard Management Controller (BMC) de American Megatrends (AMI), que podrían conducir a la ejecución remota de código en servidores vulnerables.

> *«El impacto de explotar estas vulnerabilidades incluye el control remoto de servidores comprometidos, la implementación remota del malware, ransomware e implante de firmware, y daños físicos al servidor (bloqueo)»,* dijo la empresa de seguridad Eclypsium.

Los BMC son sistemas independientes privilegiados dentro de servidores que se usan para controlar configuraciones de hardware de bajo nivel y administrar el sistema operativo host, incluso en escenarios cuando la máquina está apagada.

Estas capacidades hacen que los BMC sean un objetivo atractivo para los atacantes que buscan plantar malware persistente en dispositivos que puedan sobrevivir a las reinstalaciones del sistema operativo y los reemplazos del disco duro.

Llamados colectivamente BMC&C, los problemas recientemente identificados pueden ser explotados por atacantes que tienen acceso a interfaces de administración remota (IPMI) como Redfish, lo que potencialmente permite a los hackers obtener el control de los sistemas y poner en riesgo las infraestructuras de la nube.

El más grave de los problemas es CVE-2022-40259 (puntuación CVSS: 9.9), un caso de ejecución de código arbitrario a través de la API de Redfish que requiere que el atacante ya tenga un nivel mínimo de acceso en el dispositivo (privilegios de devolución de llamada o superior).

CVE-2022-40242 (puntuación CVSS: 8.3) se relaciona con un hash para un usuario administrador del sistema que se puede descifrar y abusar para obtener acceso de shell administrativo, mientras que CVE-2022-2827 (puntuaión CVSS: 7.5) es un error en el restablecimiento de contraseña, función que puede aprovecharse para determinar si existe

una cuenta con un nombre de usuario específico.

> *«[CVE-2022-2827] permite identificar usuarios preexistentes y no conduce a un caparazón, pero proporcionaría al atacante una lista de objetivos para ataques de fuerza bruta o de relleno de credenciales»,* explicaron los investigadores.

Los hallazgos subrayan una vez más la importancia de asegurar la cadena de suministro de firmware y garantizar que los sistemas BMC no estén expuestos directamente a Internet.

> *«Como los centros de datos tienden a estandarizarse en plataformas de hardware específicas, cualquier vulnerabilidad de nivel BMC probablemente se aplicaría a una gran cantidad de dispositivos y podría afectar potencialmente a todo un centro de datos y los servicios que ofrece»,* dijo la compañía.

Los hallazgos surgen cuando Binarly reveló múltiples vulnerabilidades de alto impacto en dispositivos basados en AMI que podrían provocar daños en la memoria y la ejecución de código arbitrario durante las primeras fases de arranque (es decir, un entorno anterior a EFI).

A principios de mayo, Eclypsium también descubrió lo que se llama una falla BMC *«Pantalones caídos»* que afecta a los servidores de Quanta Cloud Technology (QCT), una explotación exitosa de la cual podría otorgar a los atacantes el control total sobre los dispositivos.