Se han revelado dos nuevas vulnerabilidades de seguridad en el software del Controlador de Administración de Placa Base (BMC) de AMI MegaRAC que, si se explotan con éxito, podrían permitir a los actores de amenazas tomar el control remoto de servidores vulnerables e instalar malware.

> *«Estas nuevas debilidades varían en su gravedad, desde alta a crítica, e incluyen ejecución remota de código sin autenticación y acceso no autorizado al dispositivo con permisos de superusuario»*, informaron los investigadores de Eclypsium, Vlad Babkin y Scott Scheferman, en un informe compartido con Masterhacks.

> *«Estas vulnerabilidades pueden ser explotadas por atacantes remotos que tienen acceso a interfaces de gestión remota Redfish, o desde un sistema operativo de host comprometido.»*

Para empeorar las cosas, estas deficiencias también podrían ser utilizadas para instalar implantes de firmware persistentes que son inmunes a reinstalaciones del sistema operativo y reemplazos de disco duro, dañar componentes de la placa base, causar daños físicos a través de ataques de sobrevoltaje e inducir bucles de reinicio indefinidos.

> *«Los investigadores señalan que a medida que los atacantes desplazan su enfoque desde los sistemas operativos dirigidos a los usuarios hacia el código incrustado de nivel inferior en el que confía el hardware y la seguridad informática, se vuelve cada vez más difícil detectar y solucionar las vulnerabilidades.»*

Los hallazgos de Eclypsium se basan en un análisis del firmware de AMI que fue filtrado en un ataque de ransomware realizado por el grupo RansomExx, apuntando al fabricante de hardware GIGABYTE en agosto de 2021.

Las vulnerabilidades son las últimas incorporaciones a un conjunto de fallas que afectan a los BMC MegaRAC de AMI, que han sido agrupadas bajo el nombre de BMC&C, algunas de las cuales fueron reveladas por la empresa de seguridad de firmware en diciembre de 2022 (CVE-2022-40259, CVE-2022-40242 y CVE-2022-2827) y en enero de 2023 (CVE-2022-26872 y CVE-2022-40258).

La lista de nuevas debilidades es la siguiente:

- CVE-2023-34329 (puntuación CVSS: 9.1) – Bypass de autenticación a través de manipulación de encabezados HTTP.
- CVE-2023-34330 (puntuación CVSS: 8.2) – Inyección de código a través de la interfaz de extensión dinámica Redfish.

Cuando se combinan, estas dos fallas tienen una puntuación de gravedad combinada de 10.0, lo que permitiría a un atacante evitar la autenticación de Redfish y ejecutar código arbitrario en el chip BMC de forma remota con los máximos privilegios. Además, las vulnerabilidades mencionadas podrían combinarse con CVE-2022-40258 para descifrar contraseñas de cuentas de administrador en el chip BMC.

Es importante señalar que un ataque de este tipo podría resultar en la instalación de malware que permitiría realizar espionaje cibernético a largo plazo, pasando desapercibido para el software de seguridad, sin mencionar la posibilidad de realizar movimientos laterales e incluso dañar la CPU mediante técnicas de manipulación de administración de energía, como PMFault.

Aunque no hay evidencia de que las fallas hayan sido explotadas en la práctica, la popularidad del BMC MegaRAC, un componente crítico en la cadena de suministro presente en millones de dispositivos enviados por importantes fabricantes, lo convierte en un objetivo lucrativo para los actores de amenazas que buscan controlar cada aspecto del sistema objetivo.

> *«Estas vulnerabilidades representan un riesgo importante para la cadena de suministro tecnológico que sustenta la computación en la nube. En resumen, las vulnerabilidades en un proveedor de componentes afectan a muchos fabricantes de hardware, lo que a su vez puede tener un impacto en muchos servicios en la nube»*, señalan los investigadores.

> *«Por tanto, estas vulnerabilidades pueden suponer un riesgo tanto para los servidores y el hardware de una organización directamente, como para el hardware que respalda los servicios en la nube que utilizan».*