Se han divulgado diversas debilidades de seguridad en el firmware de la Interfaz de Gestión de Plataforma Inteligente (IPMI) correspondiente a los controladores de administración de la placa base (BMC) de Supermicro, lo cual podría conducir a un aumento de privilegios y la ejecución de código malicioso en los sistemas afectados.

Estas siete vulnerabilidades, identificadas desde CVE-2023-40284 hasta CVE-2023-40290, presentan grados de severidad que varían desde Alto hasta Crítico, según Binarly. Esto habilita a actores no autenticados para obtener acceso de administrador en el sistema BMC. Supermicro ha lanzado una actualización de firmware BMC para corregir estos problemas de seguridad.

Los BMC son procesadores especiales emplazados en las placas base de los servidores, y respaldan la administración remota, permitiendo a los administradores supervisar indicadores de hardware, como la temperatura, ajustar la velocidad de los ventiladores y actualizar el firmware del sistema UEFI. Además, los chips BMC siguen operativos incluso si el sistema operativo principal está desconectado, lo que los convierte en objetivos atractivos para desplegar malware persistente.

A continuación, se ofrece una breve explicación de cada una de las vulnerabilidades:

- CVE-2023-40284, CVE-2023-40287 y CVE-2023-40288 (puntuación CVSS: 9.6) – Tres deficiencias de secuencias de comandos entre sitios (XSS) que posibilitan que atacantes remotos y no autenticados ejecuten código JavaScript arbitrario en el contexto del usuario BMC autenticado.
- CVE-2023-40285 y CVE-2023-40286 (puntuación CVSS: 8.6) – Dos deficiencias de secuencias de comandos entre sitios (XSS) que permiten a atacantes remotos y no autenticados ejecutar código JavaScript arbitrario en el contexto del usuario BMC autenticado al manipular las cookies del navegador o el almacenamiento local.
- CVE-2023-40289 (puntuación CVSS: 9.1) – Una falla de inyección de comandos en el sistema operativo que permite la ejecución de código malicioso con privilegios de administrador.
- CVE-2023-40290 (puntuación CVSS: 8.3) – Una deficiencia de secuencias de comandos

> entre sitios (XSS) que permite a atacantes remotos y no autenticados ejecutar código JavaScript arbitrario en el contexto del usuario BMC autenticado, pero solo cuando se utiliza el navegador Internet Explorer 11 en Windows.

Según Binarly, CVE-2023-40289 es *«crítico porque permite a atacantes autenticados obtener acceso de administrador y comprometer completamente el sistema BMC».*

> *«Este nivel de acceso permite llevar a cabo ataques persistentes incluso después de reiniciar el componente BMC y moverse lateralmente dentro de la infraestructura comprometida, infectando otros dispositivos».*

Las otras seis vulnerabilidades, especialmente CVE-2023-40284, CVE-2023-40287 y CVE-2023-40288, podrían ser empleadas para crear una cuenta con privilegios de administrador en el componente de servidor web del software IPMI BMC.

Como resultado, un atacante remoto que busque obtener el control de los servidores podría combinar estas vulnerabilidades con CVE-2023-40289 para llevar a cabo una inyección de comandos y lograr la ejecución de código. En un escenario hipotético, esto podría manifestarse como el envío de un correo electrónico de phishing con un enlace malicioso a la dirección de correo electrónico del administrador. Al hacer clic en el enlace, se activaría la ejecución de la carga útil de XSS.

Actualmente, no se ha encontrado evidencia de explotación maliciosa de estas vulnerabilidades en la naturaleza. Sin embargo, Binarly informó que observó más de 70,000 instancias de interfaces web IPMI de Supermicro expuestas en Internet a principios de octubre de 2023.

> *«En primer lugar, es posible comprometer el sistema BMC de forma remota explotando vulnerabilidades en el componente del servidor web expuesto en Internet»,* explicó la empresa de seguridad de firmware.

> *«Luego, un atacante puede obtener acceso al sistema operativo del servidor mediante la funcionalidad legítima de BMC de control remoto iKVM o al actualizar el firmware UEFI del sistema objetivo con firmware malicioso que permite el control persistente del sistema operativo principal. A partir de ahí, nada impide que un atacante se desplace lateralmente dentro de la red interna y comprometa otros dispositivos».*

A principios de este año, se descubrieron dos debilidades de seguridad en los BMC MegaRAC de AMI que, si se explotaran con éxito, podrían permitir que actores de amenazas tomaran el control de servidores vulnerables y desplegaran malware.