Los servidores de Quata Cloud Technology (QCT), fueron identificados como vulnerables a la grave falla del controlador de administración de placa base (BMC) *«Pantsdown»*, según una investigación publicada la semana pasada.

> *«Un atacante que ejecute código en un servidor QCT vulnerable podría 'saltar' del host del servidor al BMC y mover sus ataques a la red de administración del servidor, posiblemente continuar y obtener más permisos para otros BMC en la red y al hacerlo, obtener acceso a otros servidores»*, dijo la compañía de seguridad Eclypsium.

Un controlador de gestión de placa base es un sistema especializado que se utiliza para la supervisión y gestión remotas de servidores, incluyendo el control de configuraciones de hardware de bajo nivel, así como la instalación de actualizaciones de firmware y software.

Rastreada como CVE-2019-6220, con puntaje CVSS de 9.8, la vulnerabilidad crítica salió a la luz en enero de 2019, y se relaciona con un caso de acceso arbitrario de lectura y escritura al espacio de direcciones físicas de BMC, lo que resultó en la ejecución de código arbitrario.

La explotación exitosa de la vulnerabilidad puede proporcionar a un actor de amenazas un control total sobre el servidor, lo que permite sobrescribir el firmware de BMC con código malicioso, implementar malware persistente, filtrar datos e incluso bloquear el sistema.

Los modelos de servidor QCT afectados incluyen D52BQ-2U, D52BQ-2U 3UPI, D52BV-2U, que vienen con BMC versión 4.55.00 que ejecuta una versión del software BMC vulnerable a Pantsdown. Luego de la divulgación responsable el 7 de octubre de 2021, un parche se puso a disposición de los clientes de forma privada el 15 de abril.

El hecho de que aún exista una debilidad de tres años subraya la necesidad de fortalecer el código de nivel de firmware aplicando actualizaciones de forma oportuna y escaneando regularmente el firmware en busca de posibles indicadores de compromiso.

La seguridad del firmware es particularmente crucial a la luz del hecho de que componentes como BMC se convirtieron en un objetivo lucrativo de ataques cibernéticos destinados a plantar malware sigiloso como iLOBleed, que está diseñado para borrar por completo los discos del servidor de la víctima.

Para mitigar los riesgos, se recuerda que las organizaciones que confían en los productos QCT deben verificar la integridad de su firmware BMC y actualizar el componente a la última versión a medida que las correcciones estén disponibles.

> *«Los adversarios se sienten cada vez más cómodos con ataques a nivel de firmware. Lo que es importante tener en cuenta es cómo ha aumentado el conocimiento de las vulnerabilidades a nivel de firmware a lo largo de los años: lo que era difícil en 2019 es casi trivial hoy»,* dijo la compañía.