Se han descubierto múltiples vulnerabilidades de seguridad en varios servicios, incluyendo el sistema de control distribuido (DCS) Honeywell Experion y QuickBlox, que, en caso de ser explotadas exitosamente, podrían resultar en un compromiso severo de los sistemas afectados.

Conocidas como Crit.IX, las nueve fallas en la plataforma Honeywell Experion DCS permiten la *«ejecución remota de código no autorizada, lo que significa que un atacante tendría la capacidad de tomar el control de los dispositivos y modificar el funcionamiento del controlador DCS, al mismo tiempo que oculta las modificaciones al equipo de ingeniería encargado del controlador»,* mencionó Armis en un comunicado.

En otras palabras, los problemas están relacionados con la falta de encriptación y mecanismos de autenticación adecuados en un protocolo propietario llamado Control Data Access (CDA) que se utiliza para la comunicación entre los servidores Experion y los controladores C300, lo cual permite que un actor malicioso tome el control de los dispositivos y altere el funcionamiento del controlador DCS.

> *«Como resultado, cualquier persona con acceso a la red puede hacerse pasar tanto por el controlador como por el servidor. Además, existen fallos de diseño en el protocolo CDA que dificultan el control de los límites de los datos y pueden provocar desbordamientos de memoria intermedia»*, señaló Tom Gol, CTO de investigación en Armis.

La Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA), en su propio aviso, indicó que siete de las nueve fallas tienen una puntuación CVSS de 9.8 sobre 10, mientras que las otras dos tienen una calificación de gravedad de 7.5. *«La explotación exitosa de estas vulnerabilidades podría causar una condición de denegación de servicio, permitir la escalada de privilegios o permitir la ejecución remota de código»,* advirtió.

En un desarrollo relacionado, Check Point y Claroty descubrieron importantes fallas en una plataforma de chat y video llamadas conocida como QuickBlox, que se utiliza ampliamente

en telemedicina, finanzas y dispositivos inteligentes de IoT. Las vulnerabilidades podrían permitir que los atacantes filtren la base de datos de usuarios de muchas aplicaciones populares que incorporan el SDK y la API de QuickBlox.

Esto incluye a Rozcom, un proveedor israelí que vende sistemas de intercomunicación para casos de uso residenciales y comerciales. Un análisis más detallado de su aplicación móvil llevó al descubrimiento de fallas adicionales (CVE-2023-31184 y CVE-2023-31185) que permitieron la descarga de todas las bases de datos de usuarios, suplantar a cualquier usuario y llevar a cabo ataques de toma completa de cuentas.

> *«Como resultado, pudimos tomar el control de todos los dispositivos de intercomunicación de Rozcom, lo que nos brindó control total y nos permitió acceder a las cámaras y micrófonos de los dispositivos, interceptar su transmisión, abrir puertas controladas por los dispositivos y más»*, afirmaron los investigadores.

También se revelaron esta semana fallas de ejecución remota de código que afectan a los puntos de acceso de Aerohive/Extreme Networks que ejecutan versiones anteriores a 10.6r2 de HiveOS/Extreme IQ Engine, así como a la biblioteca de código abierto Ghostscript (CVE-2023-36664, puntuación CVSS: 9.8), lo cual podría resultar en la ejecución de comandos arbitrarios.

> *«Ghostscript es un paquete ampliamente utilizado pero no necesariamente conocido en gran medida. Puede ser ejecutado de múltiples formas, desde abrir un archivo en un editor de imágenes vectoriales como Inkscape hasta imprimir un archivo a través de CUPS. Esto significa que la explotación de una vulnerabilidad en Ghostscript no se limita a una sola aplicación ni es inmediatamente evidente»*, señaló el investigador de Kroll, Dave Truman

También se han revelado deficiencias de seguridad en dos plataformas de código abierto

basadas en Golang, Owncast (CVE-2023-3188, puntuación CVSS: 6.5) y EaseProbe (CVE-2023-33967, puntuación CVSS: 9.8), que podrían allanar el camino para ataques de falsificación de solicitudes en el lado del servidor (SSRF) e inyección de SQL, respectivamente.

Para completar la lista, se ha descubierto el uso de credenciales codificadas de forma estática en los enrutadores Technicolor TG670 DSL, lo que permitiría a un usuario autenticado obtener un control administrativo completo sobre los dispositivos.

> *«Un atacante remoto puede utilizar el nombre de usuario y la contraseña predeterminados para iniciar sesión como administrador en el dispositivo del enrutador. Esto permite al atacante modificar cualquier configuración administrativa del enrutador y utilizarlo de formas inesperadas»*, advirtió CERT/CC en un aviso.

Se recomienda a los usuarios deshabilitar la administración remota en sus dispositivos para evitar posibles intentos de explotación y consultar con los proveedores de servicios para verificar si están disponibles los parches y las actualizaciones adecuadas.