Se revelaron alrededor de cinco docenas de vulnerabilidades de seguridad en dispositivos de 10 proveedores de tecnología operativa (OT), esto debido a lo que los investigadores de seguridad cibernética denominan *«prácticas inseguras por diseño».*

Nombradas colectivamente como OT:ICEFALL por Forescout, las 56 vulnerabilidades abarcan 26 modelos de dispositivos de Bently Nevada, Emerson, Honeywell, JTEKT, Motorola, Omron, Phoenix Contact, Siemens y Yokogawa.

> *«Al explotar estas vulnerabilidades, los atacantes con acceso a la red a un dispositivo de destino podrían ejecutar código de forma remota, cambiar la lógica, los archivos o el firmware de los dispositivos OT, eludir la autenticación, comprometer las credenciales, causar denegaciones de servicio o tener una variedad de impactos operativos»,* dijo la compañía en un informe técnico.

Las vulnerabilidades podrían tener consecuencias desastrosas considerando que los productos afectados se emplean ampliamente en industrias de infraestructura crítica como petróleo y gas, química, nuclear, generación y distribución de energía, fabricación, tratamiento y distribución de agua, minería y automatización de edificios.

De las 56 vulnerabilidades descubiertas, el 38% permite el compromiso de las credenciales, el 21% permite la manipulación del firmware, el 14% permite la ejecución remota de código y el 8% de las fallas permite la manipulación de la información de configuración.

Además de permitir potencialmente que un atacante suministre código arbitrario y realice modificaciones no autorizadas en el firmware, las vulnerabilidades también podrían aprovecharse para desconectar completamente un dispositivo y eludir las funciones de autenticación existentes para invocar cualquier funcionalidad en los objetivos.

Más importante aún, los esquemas de autenticación rotos, incluido el desvío, el uso de protocolos criptográficos riesgosos y las credenciales codificadas y de texto sin formato, representaron 22 de las 56 fallas, lo que indica *«controles de seguridad deficientes»* durante

la implementación.

En un escenario hipotético del mundo real, estas deficiencias podrían utilizarse como armas contra tuberías de gas natural, turbinas eólicas o líneas de ensamblaje de fabricación discreta para interrumpir el transporte de combustible, anular las configuraciones de seguridad, detener la capacidad de controlar las estaciones de compresión y alterar el funcionamiento de la lógica programable de controladores (PLC).

Pero las amenazas no son solo teóricas. Una falla de ejecución remota de código que afectaba a los controladores Omron NJ/NX (CVE-2022-31206) fue, en realidad, explotada por un atacante alineado con el estado llamado CHERNOVITE para desarrollar una parte de un malware sofisticado llamado PIPEDREAM (también conocido como INCONTROLLER).

La creciente interconexión entre las redes de TI y OT complica la gestión de riesgos, junto con la naturaleza opaca y propietaria de muchos sistemas de OT, sin mencionar la ausencia de CVE, lo que hace las vulnerabilidades persistentes sean invisibles, así como la retención de características inseguras por diseño para mucho tiempo.

Como medida de mitigación para OT:ICEFALL, se recomienda descubrir e inventariar dispositivos vulnerables, aplicar parches específicos del proveedor, hacer cumplir la segmentación de activos de OT, monitorear el tráfico de red en busca de actividad maliciosa y adquirir productos seguros por diseño para reforzar la cadena de suministro.

> *«El desarrollo de malware reciente dirigido a la infraestructura crítica, como Industroyer2, Triton e INCONTROLLER, ha demostrado que los atacantes son conscientes de la naturaleza insegura del diseño de la tecnología operativa y están listos para explotarlas y causar estragos»,* dijeron los investigadores.

> *«A pesar del importante papel que juegan los esfuerzos de fortalecimiento basados en estándares en la seguridad de OT, los productos con características inseguras por diseño y controles de seguridad quebrados trivialmente continuaron siendo certificados».*