La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó ocho avisos de Sistemas de Control Industrial (ICS) el martes, advirtiendo sobre vulnerabilidades críticas que afectan a los equipos de Delta Electronics y Rockwell Automation.

Los problemas incluyen 13 vulnerabilidades de seguridad en InfraSuite Device Master de Delta Electronics, un software de monitoreo de dispositivos en tiempo real. Todas las versiones anteriores a la 1.0.5 se ven afectadas por los problemas.

> *«La explotación exitosa de las vulnerabilidades podría permitir que un atacante no autenticado obtenga acceso a archivos y credenciales, aumente los privilegios y ejecute código arbitrario de forma remota»,* dijo CISA.

La primera vulnerabilidad de la lista es CVE-2023-1133 (puntaje CVSS: 9.8), una falla crítica que surge del hecho de que InfraSuite Device Master acepta paquetes UDP no verificados y deserializa el contenido, lo que permite que un atacante remoto no autenticado ejceute código arbitrario.

Otras dos vulnerabilidades de deserialización, CVE-2023-1139 (puntaje CVSS: 8.8) y CVE-2023-1145 (puntaje CVSS: 7.8), podrían usarse como armas para obtener la ejecución remota de código, advirtió CISA.

A Piotr Bazydlo y un invstigador de seguridad anónimo se les atribuye el descubrimiento y la notificación de las vulnerabilidades a CISA.

Otro conjunto de vulnerabilidades se relaciona con ThinManager ThinServer de Rockwell Automation y afecta a las siguientes versiones del software de administración de servidor de protocolo de escritorio remoto (RDP) y cliente ligero:

- 6.x – 10.x
- 11.0.0 – 11.0.5

- 11.1.0 – 11.1.5
- 11.2.0 – 11.2.6
- 12.0.0 – 12.0.4
- 12.1.0 – 12.1.5, y
- 13.0.0 – 13.0.1

El más grave de los problemas es la falla de cruce de dos rutas rastreada como CVE-2023-28755 (puntaje CVSS: 9.8) y CVE-2023-28756 (puntaje CVSS: 7.5) que podría permitir que un atacante remoto no autenticado cargue archivos arbitrarios en el directorio donde está instalado ThinServer.exe.

Aún más preocupante, el atacante podría armar CVE-2023-28755 para sobrescribir archivos ejecutables existentes con versiones troyanizadas, lo que podría conducir a la ejecución remota de código.

> *«La explotación exitosa de estas vulnerabilidades podría permitir que un atacante realice potencialmente la ejecución remota de código en el sistema/dispositivo de destino o bloquear el software»,* dijo CISA.

Se recomienda a los usuarios que actualicen a las versiones 11.0.6, 11.1.6, 11.2.7, 12.0.5, 12.1.6 y 13.0.2 para mitigar las amenazas. Las versiones 6.x a 10.x de ThinManager ThinServer se han retirado, lo que requiere que los usuarios actualicen a una versión compatible.

Como solución alternativa, también se recomienda que el acceso remoto al puerto 2031/TCP se limite a clientes ligeros y servidores ThinManager conocidos.

La divulgación llega más de seis meses después de que CISA alertara sobre una vulnerabilidad de desbordamiento de búfer de alta gravedad en Rockwell Automation ThinManager ThinServer (CVE-2022-38742, puntaje CVSS: 8.1) que podría resultar en la ejecución remota de código arbitrario.