PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 14 de junio de 2022

N° 159-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 159**	**Fecha: 14-06-2022**
		Página 4 de 5

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de DoS en el puerto Ethernet del módulo CPU de las series Q y L de MELSEC de Mitsubishi Electric		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado una vulnerabilidad de severidad ALTA de tipo bloqueo de recursos inadecuado en múltiples productos de Mitsubishi Electric. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS).

2. Detalles:

- La vulnerabilidad de tipo bloqueo de recursos inadecuado se debe a que el software no bloquea o no bloquea correctamente un recurso cuando el software debe tener acceso exclusivo al recurso, un atacante podría modificar el recurso mientras el software lo utiliza. Esto podría violar la suposición del software de que el recurso no cambiará, lo que podría generar comportamientos inesperados.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-24946 de bloqueo de recursos inadecuado, existe debido a un bloqueo inadecuado de los recursos (falta de liberación de recursos). Un atacante malintencionado puede causar una condición DoS en las comunicaciones Ethernet mediante el envío de un paquete especialmente diseñado. Se requiere un restablecimiento del sistema de los productos para la recuperación.

3. Productos afectados:

- Q03UDECPU y Q04/06/10/13/20/26/50/100UDEHCPU, todas las versiones;
- Productos con los primeros 5 dígitos del número de serie "24051" y anteriores de:
  - ✓ Q03/04/06/13/26UDVCPU;
  - ✓ Q04/06/13/26UDPVCPU;
  - ✓ L02/06/26CPU(-P), L26CPU-(P)BT.

4. Solución:

- Mitsubishi Electric recomienda actualizar los módulos que comiencen con los primeros 5 dígitos del número de serie "24052" y posteriores de los productos:
  - ✓ Q03/04/06/13/26UDVCPU;
  - ✓ Q04/06/13/26UDPVCPU;
  - ✓ L02/06/26CPU(-P), L26CPU-(P)BT;
- Asimismo, exhorta a tomar las siguientes medidas de mitigación para minimizar el riesgo de explotación de esta vulnerabilidad:
  - ✓ Utilizar un firewall o una red privada virtual (VPN), etc. para evitar el acceso no autorizado cuando se requiera acceso a Internet;
  - ✓ Uso dentro de una LAN y bloqueo del acceso desde redes y hosts que no son de confianza a través de firewalls.

Fuentes de información	▪ hxxps://www.incibe-cert.es/alerta-temprana/avisos-sci/denegacion-servicio-productos-mitsubishi-electric-0 ▪ hxxps://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-007_en.pdf

Índice alfabético