DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 129**	**Fecha: 02-06-2023**
		Página 12 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el entorno de alojamiento de aplicaciones Cisco IOX		
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:**

Cisco ha reportado una vulnerabilidad de severidad ALTA de tipo inyección de comandos del entorno de alojamiento de aplicaciones que afecta a Cisco IOX. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios como root en el sistema operativo host subyacente.

2. Detalles:

- La vulnerabilidad registrada con el código CVE-2023-20076 de severidad **alta** de tipo inyección de comandos en el entorno de alojamiento de aplicaciones Cisco IOx podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios como root en el sistema operativo host subyacente.

- Esta vulnerabilidad se debe a una sanitización incompleta de los parámetros que se pasan para la activación de una aplicación. Un atacante podría aprovechar esta vulnerabilidad al implementar y activar una aplicación en el entorno de alojamiento de aplicaciones Cisco IOx con un archivo de carga útil de activación manipulado. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios como root en el sistema operativo host subyacente.

3. Productos afectados:

- Dispositivos Cisco que ejecutan el software Cisco IOS XE si tienen habilitada la función Cisco IOx y no admiten la ventana acoplable nativa;
- Asimismo, afecta a los productos que no son compatibles con la ventana acoplable nativa, si ejecutan una versión de software vulnerable y habilita la función Cisco IOx:
  - ISR industriales de la serie 800;
  - Módulos de computo CGR 1000;
  - Gateways de computo industrial IC3000 (las versiones 1.2.1 y posteriores);
  - Enrutadores industriales WPAN IR510.

4. Solución:

- Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

Fuentes de información	▪ hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL