Nro. Alerta:	EC-2022-0XX	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	1X-ago-2022	VULNERABILIDAD REALTEK eCOS SDK	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de vulnerabilidad: CVE-2022-27255
Nivel de riesgo: Alto

II. ALERTA

El grupo de expertos de seguridad de Faraday descubrió una vulnerabilidad crítica que afecta al eCos SDK fabricado por la empresa taiwanesa de semiconductores Realtek, la cual podría exponer los dispositivos de red de varios proveedores a ataques remotos.

La falla identificada con el CVE-2022-27255, es un desbordamiento de búfer basado en pila que puede proporcionar a un atacante remoto acceso a la ejecución de código arbitrario en dispositivos que usan el SDK. Se pueden utilizar paquetes SIP especialmente diseñados para atacar la interfaz WAN.

Figura No. 1: Vulnerabilidad Realtek eCOS SDK
Fuente: Infoshare Systems

III. INTRODUCCIÓN

El Realtek eCos SDK es utilizado por las empresas que fabrican routers, access points y repetidores que utilizan la tecnología de la familia RTL819x. Como parte del SDK, se ha implementado una interfaz para la administración web y la pila de redes del router. Con el SDK, los proveedores pueden agregar funciones y marcas personalizadas a sus dispositivos, incluso la interfaz de administración web y la pila de red.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-0XX	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	1X-ago-2022	VULNERABILIDAD REALTEK eCOS SDK	V 1.1

Realtek informó a los clientes sobre la vulnerabilidad eCos SDK en marzo, cuando anunció la disponibilidad de un parche. Sin embargo, depende de los fabricantes que usen el SDK asegurarse de que el parche se distribuya a los dispositivos de los usuarios finales.

Se determinó que la vulnerabilidad se puede explotar de forma remota, para afectar los enrutadores afectados que se ejecutan con la configuración predeterminada. No se requiere interacción del usuario para que la explotación sea exitosa, por lo que, si el dispositivo está conectado a Internet, el atacante sólo necesita enviar un paquete para tomar el control del dispositivo, todo esto debido a que el código vulnerable es parte de la pila de red.

IV. VECTOR DE ATAQUE: Explotación de vulnerabilidad

V. IMPACTO:

La explotación de esta vulnerabilidad afecta a las Series: Realtek rtl819x-eCos-v0.x y rtl819x-eCos-v1.x.

VI. INDICADORES DE COMPROMISO:

No aplica.

VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- Aplicar los parches de seguridad en los enrutadores fabricados con versiones vulnerables del SDK de Realtek eCos.
- Se debe verificar que todas las aplicaciones, bases de datos, servidores y dispositivos de red se estén configurados adecuadamente.
- Realizar evaluaciones periódicas de la seguridad para el fortalecimiento de la infraestructura y activos críticos expuestos a Internet.
- Realizar regularmente copias de seguridad de las aplicaciones, las bases de datos y todos los datos críticos.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-0XX	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	1X-ago-2022	VULNERABILIDAD REALTEK eCOS SDK	V 1.1

VIII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *Realtek SDK Vulnerability Exposes Routers From Many Vendors to Remote Attacks | SecurityWeek.Com*. (s. f.). SecurityWeek - A Wired Business Media Publication. Recuperado 19 de agosto de 2022, de https://www.securityweek.com/realtek-sdk-vulnerability-exposes-routers-many-vendors-remote-attacks.

- Post, C. T. (2022, 17 agosto). *Realtek eCos SDK Vulnerability Expose Multiple Routers to Remote Attacks*. Cyber Threat Post & Advisory. Recuperado 19 de agosto de 2022, de https://varutra.com/ctp/posts/postDetails/R3VDTDdxUkVEbDFDSWQ4WVJpU0ROdz09/Realtek-eCos-SDK-Vulnerability-Expose-Multiple-Routers-to-Remote-Attacks.

- Agrawal, S. (2022, 14 agosto). *Due to a Realtek SDK weakness, routers from various vendors are exposed to remote assaults*. The Tech Outlook. Recuperado 19 de agosto de 2022, de https://www.thetechoutlook.com/news/technology/security/due-to-a-realtek-sdk-weakness-routers-from-various-vendors-are-exposed-to-remote-assaults/.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec