Nro. Alerta:	EC-2022-27	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	10-febrero-2022	**Vulnerabilidad en TP-Link TL-WR841N**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alto

II. ALERTA

Una vulnerabilidad existente en el router inalámbrico TP-Link TL-WR841N ha sido identificada con el CVE-2022-0162; dando la posibilidad que un atacante acceda a la interfaz de administración Web del dispositivo afectado con privilegios de administrador.

Figura 1. Ilustración asociada al router inalámbrico TP LINK TL-WR841N
Fuente: TP LINK

III. INTRODUCCIÓN

El router inalámbrico TP-Link TL-WR841N transmite la información de autenticación sin emplear ningún tipo de encriptación[1], únicamente hace uso de una codificación[2] base64; es decir emplea **cleartextbase64.**

En este sentido, el grupo de investigación de Veermata Jijabai Technological Institute (VJTI Mumbai) dio a conocer una vulnerabilidad en el router TP-Link TL-WR841N en su versión V11 3.16.9 Build 160325 Rel.62500n; específicamente en una función desconocida del

[1] Proceso técnico por el cual la información se convierte en un código secreto que permite ocultar los datos que envías. La información una vez encriptada solo puede verse aplicándole una clave que previamente deben conocer tanto el emisor como el receptor de esa información
[2] Proceso que permite convertir datos de un formato a otro formato

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

componente Web-based Management Interface, la misma que mediante la manipulación de un input desconocido causa una vulnerabilidad de clase cifrado débil.

A continuación, se mencionan características de la vulnerabilidad asociada a este equipo:

Descripción	Detalle
Fecha de publicación de CVE	10 de febrero de 2022
CVE asignado	CVE-2022-0162
Versiones afectadas	V11 3.16.9 Build 160325 Rel.62500n
Puntuación CVSS	8.4

Tabla 1. Características generales de la vulnerabilidad.

IV. VECTOR DE ATAQUE:

La vulnerabilidad se presenta en el manejo del componente Web-based Management Interface; permitiendo que un atacante remoto intercepte las credenciales y, posteriormente, realice operaciones administrativas en el dispositivo afectado a través de la interfaz de administración basada en la web.

V. IMPACTO:

La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto intercepte las credenciales y, posteriormente, realice operaciones administrativas en el dispositivo afectado a través de la interfaz de administración basada en la web; dando como resultado una pérdida total de confidencialidad originando que todos los recursos dentro del componente afectado se divulguen al atacante; de igual manera ocurre con la integridad, provocando que el atacante pueda modificar archivos, finalmente en referencia a la disponibilidad es altamente comprometida dando como resultado que el atacante pueda denegar el acceso a los recursos del componente afectado.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar programas y archivos de fuentes oficiales.
- Revisar continuamente si el fabricante del equipo dispone de actualizaciones y actualizar el firmware de TPlink WR841N.
- Deshabilitar las funciones de administración remota de su dispositivo.

Nro. Alerta:	EC-2022-27	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	10-febrero-2022	**Vulnerabilidad en TP-Link TL-WR841N**	Versión 1.0

VII. REFERENCIAS:

CertIN. (07 de 02 de 2022). *CertIN*. Obtenido de CertIN: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2022-0068

HYPR. (s.f.). *HYPR*. Obtenido de HYPR: https://www.hypr.com/cleartext/

LINK, T. (s.f.). *TP LINK*. Obtenido de TP LINK: https://www.tp-link.com/es/home-networking/wifi-router/tl-wr841n/

MITRE, C. (s.f.). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0162

Vuldb. (10 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.192649