Nro. Alerta:	EC-2022-13	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	25-enero-2022	**Vulnerabilidad en el manejo de las respuestas DNS en los A.P. " TP-Link TL-WA1201 "**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Desbordamiento de búfer basado en pila (Stack)
Nivel de riesgo: Medio

II. ALERTA

Una vulnerabilidad ha sido detectada en los puntos de acceso inalámbrico TP-Link TL-WA1201; específicamente se presentan fallos en el manejo de respuestas de DNS lo que conlleva a generación de un desbordamiento de un búfer de longitud fija en la región stack de memoria; así mismo, el atacante puede ejecutar código en el contexto de root.

Figura 1.- Ilustración asociada al AP TL-WA1201
Fuente: TPLINK

III. INTRODUCCIÓN

El 18 de junio de 2020 TP-LINK anunció la disponibilidad del Punto de Acceso Inalámbrico TL-WA1201; este producto permite mejorar la conectividad a nivel de hogar y oficinas pequeñas; sin embargo, el 16 de septiembre de 2021 se reportó al fabricante una

Nro. Alerta:	EC-2022-13	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	25-enero-2022	**Vulnerabilidad en el manejo de las respuestas DNS en los A.P. " TP-Link TL-WA1201 "**	Versión 1.0

vulnerabilidad asociada a este producto y en el presente año se la asignó la CVE correspondiente.

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

Descripción	Detalle
Fecha de publicación de CVE	17 de enero de 2022
CVE asociado	CVE-2021-35004
Versiones afectadas	1.0.1 Build 20200709 rel.66244(5553)
Puntuación CVSS	8.8

Tabla 1. Características generales de la vulnerabilidad.

IV. VECTOR DE ATAQUE: REMOTO

La vulnerabilidad se presenta en el manejo de las respuestas DNS del equipo; y considerando que estos mensajes pueden ser diseñados e implementados de una manera específica; pueden provocar un desbordamiento de un búfer de longitud fija en la región stack de la memoria.

Finalmente, los atacantes pueden aprovechar esta vulnerabilidad para ejecutar código en el contexto de root, para explotar esta vulnerabilidad no se requiere de una autenticación.

V. IMPACTO

Existe 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:

- Revisar continuamente si el fabricante del equipo dispone de actualizaciones.
- Verificar la configuración de DNS con regularidad.
- Deshabilitar las funciones de administración remota de su dispositivo.

Nro. Alerta:	EC-2022-13	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	25-enero-2022	**Vulnerabilidad en el manejo de las respuestas DNS en los A.P. " TP-Link TL-WA1201 "**	Versión 1.0

VII. REFERENCIAS:

Agency, C. &. (24 de 01 de 2022). *CISA*. Obtenido de CISA: https://www.cisa.gov/uscert/ncas/bulletins/sb22-024

Chamberland, C. (13 de 01 de 2022). *Wordfence*. Obtenido de Wordfence: https://www.wordfence.com/blog/2022/01/84000-wordpress-sites-affected-by-three-plugins-with-the-same-vulnerability/

Fuertes, R. (20 de 01 de 2022). *Una al Día*. Obtenido de Una al Día: https://unaaldia.hispasec.com/2022/01/vulnerabilidad-critica-en-plugins-wordpress.html

Incibe-Cert. (21 de 01 de 2022). *Incibe-Cert*. Obtenido de Incibe-Cert: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-35004

Initiative, Z. D. (17 de 01 de 2022). *Zero Day Initiative*. Obtenido de Zero Day Initiative: https://www.zerodayinitiative.com/advisories/ZDI-22-081/

Lakshmanán, R. (16 de 01 de 2022). *Hacker News*. Obtenido de Hacker News: https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html?m=1

LINK, T. (s.f.). *TP LINK*. Obtenido de TP LINK: https://www.tp-link.com/ec/home-networking/access-point/tl-wa1201/

MITRE, C. (13 de 01 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0215

Security, F. o. (13 de 01 de 2022). *Forum of Incident Response and Security Teams*. Obtenido de Forum of Incident Response and Security Teams: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

TP-LINK. (18 de 06 de 2020). *TP-LINK*. Obtenido de TP-LINK: https://www.tp-link.com/es/press/news/18988/

WordPress. (s.f.). *WordPress*. Obtenido de WordPress: https://wordpress.org/