Nro. Alerta:	AL-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	13-Enero-2023	**Vulnerabilidades en el firmware de Qualcomm**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistemas Vulnerables
Nivel de riesgo: Crítico, Alto y Medio dependiendo del sistema

II. ALERTA

El boletín de seguridad de enero de 2023 de Qualcomm, abordó 22 vulnerabilidades de software en su suite Snapdragon, que afectaron los dispositivos de Microsoft, Lenovo y Samsung, entre otros.

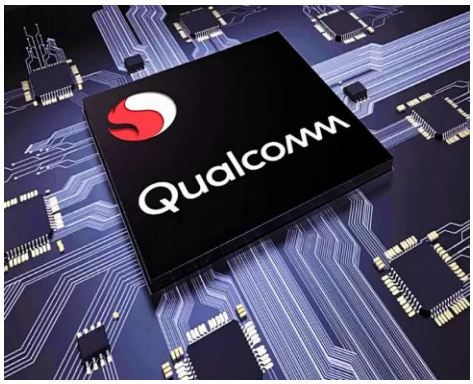

Figura 1.- Ilustración asociada a Qualcomm
Fuente: Forbes.com.ec

III. INTRODUCCIÓN

El boletín de seguridad de enero de 2023 de Qualcomm, informó 22 vulnerabilidades de software en su suite Snapdragon. Algunas de las fallas fueron reportadas por el equipo efiXplorer de la firma de protección de firmware Binarly, Zinuo Han de OPPO Amber Security Lab, Gengjia Chen de IceSword Lab, los investigadores nicolas (nicolas1993), Seonung Jang de STEALIEN y Le Wu de Baidu Security

Las vulnerabilidades de Qualcomm, algunas calificadas como de alta gravedad, se identificaron en el código de referencia del firmware de UEFI e impactan en todo el ecosistema de computadoras portátiles y dispositivos basados en ARM en chips Qualcomm Snapdragon, que son utilizados en una gran cantidad de dispositivos de distintas marcas tales como: Lenovo, Microsoft, Samsung, HP, entre otros.

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

Nro. Alerta:	AL-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	13-Enero-2023	**Vulnerabilidades en el firmware de Qualcomm**	Versión 1.0

A continuación se reportan los CVEs asociados a las vulnerabilidades, que se encuentran en el boletín:

CVE	Clasificación de seguridad	Clasificación CVSS	Área de Tecnología
CVE-2022-33218	Crítico	Alto	Automotor
CVE-2022-33219	Crítico	Crítico	Automotor
CVE-2022-33265	Crítico	Alto	Firmware de PCL (comunicación por línea eléctrica)
CVE-2022-25725	Alto	Medio	UTILIDADES
CVE-2022-25746	Alto	Alto	NÚCLEO (KERNEL)
CVE-2022-33252	Alto	Alto	Firmware de WLAN
CVE-2022-33253	Alto	Alto	Firmware de WLAN
CVE-2022-33266	Alto	Medio	Audio
CVE-2022-33274	Alto	Alto	Núcleo de Android
CVE-2022-33276	Alto	Alto	Firmware de WLAN
CVE-2022-33283	Alto	Alto	Firmware de WLAN
CVE-2022-33284	Alto	Alto	Firmware de WLAN
CVE-2022-33285	Alto	Alto	Firmware de WLAN
CVE-2022-33286	Alto	Alto	Firmware de WLAN
CVE-2022-33290	Alto	Alto	Conectividad automotriz
CVE-2022-33299	Alto	Alto	Conectividad automotriz
CVE-2022-33300	Alto	Alto	Sistema operativo Android automotriz
CVE-2022-40516	Alto	Alto	Boot (Inicio del sistema)
CVE-2022-40517	Alto	Alto	Boot (Inicio del sistema)
CVE-2022-40520	Alto	Alto	Conectividad
CVE-2022-40518	Medio	Medio	Boot (Inicio del sistema)
CVE-2022-40519	Medio	Medio	Boot (Inicio del sistema)

Tabla 1. CVEs asignadas. (Qualcomm Documentation, 2023)

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

Nro. Alerta:	AL-2023-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	13-Enero-2023	**Vulnerabilidades en el firmware de Qualcomm**	Versión 1.0

IV. VECTOR DE ATAQUE:

No se indica.

V. IMPACTO:

La falla más grave en el boletín de seguridad de Qualcomm, es el desbordamiento de la memoria (buffer overflow) en sistemas de Automotores, registrado como: CVE-2022-33219 (puntaje CVSS 9.3).

Otros dos problemas graves solucionados por Qualcomm son:

CVE-2022-33218 (puntuación CVSS 8.2): la falla es una corrupción de memoria en sistemas de automotores.

CVE-2022-33265 (puntaje CVSS 7.3): la falla es una exposición del firmware en PLCs.

VI. INDICADORES DE COMPROMISO:

La lista de chipsets de Qualcomm, que fueron afectados puede ser obtenida en el enlace indicado en la referencia “Qualcomm Documentation, 2023”

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Se sugiere revisar de manera periódica, los sitios de los fabricantes de los dispositivos utilizados, para conocer vulnerabilidades que los afectan.
- Mantener e Instalar las actualizaciones oficiales y parches de seguridad proporcionados por los fabricantes cuando se encuentren disponibles.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

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

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Ahmed, D. (2023, Enero 6). *Chip Vulnerabilities Impacting Microsoft, Lenovo, and Samsung Devices*. HackRead | Latest Cyber Crime - InfoSec- Tech - Hacking News. https://www.hackread.com/microsoft-lenovo-samsung-chip-vulnerabilities/

Binarly [Binarly]. (2023, Enero 9). *Binarly Discovers 16 New, High-Impact Vulnerabilities in Firmware Affecting HP Enterprise Devices*. www.binarly.io. Retrieved January 13, 2023, from https://www.binarly.io/news/Binarly-Discloses-Multiple-Firmware-Vulnerabilities-in-Qualcomm-and-Lenovo-ARM-based-Devices/index.html

Paganini, P. (2023, Enero 9). *Qualcomm Snapdragon flaws impact Lenovo, Microsoft, Lenovo, and Samsung devices*. Security Affairs. https://securityaffairs.com/140528/security/qualcomm-snapdragon-flaws.html?_gl=1*n7bxkp*_ga*MTUzNTU2MDMyLjE2NjM2ODUwNjE.*_ga_8ZWTX5HC4Z*MTY3MzI3MzE0Ni4yMDkuMC4xNjczMjczMTQ2LjAuMC4w*_ga_P62M3QN974*MTY3MzI3MzE0Ni4yMDkuMC4xNjczMjczMTQ2LjAuMC4w

Qualcomm Documentation. (2023). https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2023-bulletin.html

Qualcomm UEFI Flaws Expose Microsoft, Lenovo, Samsung Devices to Attacks | SecurityWeek.Com. (2023). SecurityWeek - a Wired Business Media Publication. https://www.securityweek.com/qualcomm-uefi-flaws-expose-microsoft-lenovo-samsung-devices-attacks

Wadhwani, S. (2023, Enero 11). *Qualcomm and Lenovo Fix High Severity UEFI Vulnerabilities in Chipsets*. Spiceworks. https://www.spiceworks.com/it-security/vulnerability-management/news/uefi-firmware-vulnerabilities-qualcomm-chipsets-lenovo/

Yahoo is part of the Yahoo family of brands. (2023). https://finance.yahoo.com/news/binarly-discloses-multiple-firmware-vulnerabilities-184300473.html?guccounter=1