Boletín informativo

CSIRTSALUD-AL-20260525-105

TLP: CLEAR

Alerta ID:	104
Fecha del reporte:	25/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Botnet RondoDox explota vulnerabilidad crítica en routers ASUS para secuestro masivo de dispositivos
Herramienta de detección	VulnCheck Canary Network
Activo involucrado:	Routers ASUS, dispositivos IoT, infraestructura perimetral, redes corporativas, servicios de conectividad institucional, dispositivos SOHO y entornos híbridos
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la campaña activa asociada al botnet RondoDox, la cual está explotando la vulnerabilidad crítica CVE-2018-5999 en routers ASUS para comprometer dispositivos vulnerables y utilizarlos dentro de operaciones maliciosas de denegación de servicio distribuido (DDoS), persistencia remota y expansión de infraestructura botnet.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que esta amenaza podría generar sobre:

- infraestructura perimetral institucional;
- dispositivos de red expuestos a Internet;
- conectividad entre sedes;
- servicios clínicos soportados sobre redes IP;

- disponibilidad de plataformas hospitalarias;
- continuidad operacional;
- redes Wi-Fi institucionales;
- servicios de telemedicina;
- acceso remoto corporativo;
- y seguridad de dispositivos IoT conectados a la infraestructura organizacional.

Asimismo, se busca generar conciencia sobre los riesgos asociados a:

- uso de dispositivos desactualizados;
- routers End-of-Life (EoL);
- exposición de servicios administrativos;
- configuraciones inseguras;
- credenciales débiles;
- ausencia de segmentación;
- y falta de actualización de firmware sobre infraestructura de borde.

En el contexto del sector salud, esta amenaza resulta especialmente relevante debido a la creciente dependencia tecnológica sobre:

- conectividad hospitalaria distribuida;
- servicios cloud híbridos;
- dispositivos médicos conectados;
- telemedicina;
- interoperabilidad institucional;
- redes inalámbricas corporativas;
- y plataformas críticas soportadas sobre Internet.

CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20260525-105

TLP: CLEAR

Descripción:

Investigadores de la firma VulnCheck reportaron una campaña activa del botnet RondoDox orientada a explotar la vulnerabilidad crítica CVE-2018-5999, la cual afecta múltiples routers ASUS y permite realizar modificaciones no autenticadas sobre configuraciones del dispositivo.

La vulnerabilidad posee una puntuación CVSS de 9.8/10 y permite a atacantes remotos ejecutar cambios sobre configuraciones administrativas sin requerir autenticación válida.

De acuerdo con la investigación publicada, el ataque aprovecha mecanismos internos del servicio “infosvr” presente en determinados routers ASUS vulnerables. Los atacantes manipulan el parámetro ateCommand_flag para habilitar modificaciones administrativas no autorizadas sobre el dispositivo comprometido.

Los investigadores indicaron que:

- el exploit asociado existe públicamente desde 2018;
- la explotación activa fue detectada recientemente;
- más de un millón de routers ASUS podrían encontrarse expuestos;
- y el botnet RondoDox inició actividades asociadas a esta explotación desde mayo de 2026.

RondoDox corresponde a una familia de botnets orientadas principalmente a:

- ataques DDoS;
- reclutamiento masivo de dispositivos IoT;
- explotación automatizada de vulnerabilidades;
- expansión de infraestructura maliciosa;
- y compromiso de dispositivos Linux e infraestructura perimetral.

Las evaluaciones técnicas señalan que el riesgo incrementa considerablemente en organizaciones donde existen:

- routers sin soporte;
- firmware desactualizado;
- administración remota habilitada;
- dispositivos expuestos directamente a Internet;
- ausencia de segmentación;
- infraestructura SOHO reutilizada en ambientes corporativos;
- y monitoreo limitado sobre dispositivos de borde.

Uno de los aspectos más relevantes del incidente corresponde a que los routers comprometidos pueden convertirse en infraestructura persistente utilizada para:

- campañas DDoS;
- movimiento lateral;
- exfiltración de tráfico;
- proxys maliciosos;
- ocultamiento de actividad criminal;
- distribución de malware;
- y ataques posteriores sobre redes institucionales.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad CVE-2018-5999 podría generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de los servicios institucionales soportados sobre infraestructura de red comprometida.

Uno de los principales riesgos asociados corresponde al secuestro remoto de dispositivos perimetrales institucionales, permitiendo que actores maliciosos obtengan control parcial o total sobre routers vulnerables.

En escenarios comprometidos, los atacantes podrían:

- modificar configuraciones DNS;
- redirigir tráfico institucional;
- interceptar comunicaciones;
- desplegar malware adicional;
- alterar reglas de red;
- comprometer sesiones administrativas;
- y facilitar persistencia remota.

Adicionalmente, los dispositivos comprometidos podrían ser incorporados dentro de botnets utilizadas para:

- ataques DDoS masivos;
- campañas coordinadas;
- abuso de infraestructura institucional;
- ocultamiento de tráfico malicioso;
- y operaciones distribuidas contra terceros objetivos.

Otro riesgo crítico corresponde a la posibilidad de afectación sobre servicios clínicos y hospitalarios dependientes de conectividad IP, incluyendo:

- plataformas HIS;
- aplicaciones clínicas;
- telemedicina;
- servicios interoperables;
- autenticación centralizada;
- VPN institucionales;
- y servicios cloud críticos.

La exposición de routers institucionales también podría facilitar:

- robo de credenciales;
- inspección de tráfico;

- ataques Man-in-the-Middle;
- propagación de malware;
- abuso de servicios internos;
- y expansión lateral dentro de redes corporativas.

En organizaciones del sector salud, este escenario representa un riesgo elevado debido a la creciente integración entre:

- redes clínicas;
- infraestructura IoT médica;
- servicios cloud;
- conectividad distribuida;
- sedes remotas;
- y dispositivos médicos conectados.

La explotación sostenida de este tipo de vulnerabilidades podría derivar en:

- indisponibilidad operacional;
- degradación de servicios hospitalarios;
- interrupción de conectividad;
- afectación de continuidad del negocio;
- pérdida de integridad de comunicaciones;
- y aumento significativo de superficie de ataque institucional.

Modo de explotación del ataque

Fase 1 – Identificación de dispositivos ASUS expuestos

El proceso de explotación inicia cuando los operadores del botnet realizan escaneo masivo de dispositivos ASUS accesibles desde Internet.

Durante esta etapa, los atacantes buscan identificar:

- routers vulnerables;
- servicios infosvr expuestos;
- modelos sin soporte;
- interfaces administrativas;
- servicios remotos habilitados;
- y firmware vulnerable.

Fase 2 – Explotación de CVE-2018-5999

Posteriormente, el atacante utiliza solicitudes especialmente diseñadas para manipular configuraciones internas del router sin requerir autenticación válida.

La explotación aprovecha debilidades presentes en:

- validación de autenticación;
- mecanismos administrativos;
- exposición de servicios internos;
- y controles insuficientes sobre configuración remota.

Durante esta fase, el atacante podría:

- cambiar contraseñas administrativas;
- habilitar acceso remoto;
- modificar DNS;
- alterar reglas de red;
- crear persistencia;
- y preparar el dispositivo para incorporación al botnet.

Fase 3 – Incorporación al botnet RondoDox

Una vez comprometido el dispositivo, el router es integrado dentro de la infraestructura del botnet.

Los operadores podrían utilizar el equipo para:

- ataques DDoS;
- relay de tráfico;
- campañas automatizadas;
- ocultamiento de origen;
- distribución de malware;
- y explotación de otros dispositivos.

RondoDox mantiene características similares a otras familias de botnets orientadas a IoT y Linux, incluyendo automatización masiva y explotación continua de vulnerabilidades conocidas.

Fase 4 – Persistencia y ocultamiento

Posteriormente, los atacantes podrían intentar mantener acceso persistente al dispositivo mediante:

- modificación de configuraciones;
- alteración de firmware;
- creación de accesos ocultos;
- cambios DNS persistentes;
- y manipulación de servicios administrativos.

En muchos escenarios, las organizaciones no detectan rápidamente este tipo de compromisos debido a que los routers continúan funcionando aparentemente de forma normal.

Fase 5 – Expansión y afectación operacional

Finalmente, el dispositivo comprometido puede utilizarse como punto de apoyo para:

- movimiento lateral;
- espionaje de tráfico;
- ataques internos;
- interrupción de servicios;
- afectación de conectividad;
- sabotaje operacional;
- y compromiso progresivo de infraestructura institucional.

En el contexto del sector salud, este escenario podría impactar directamente:

- plataformas clínicas;
- servicios hospitalarios digitales;
- sistemas administrativos;
- autenticación remota;
- conectividad entre sedes;
- y continuidad operacional.

Vulnerabilidades asociadas

Exposición de dispositivos perimetrales sin actualización

- **Descripción:** La vulnerabilidad CVE-2018-5999 evidencia los riesgos asociados al uso prolongado de routers ASUS vulnerables y desactualizados dentro de infraestructuras institucionales. Muchos dispositivos afectados continúan operando con firmware antiguo debido a ausencia de gestión de actualizaciones, limitaciones operacionales,

desconocimiento del riesgo, uso de infraestructura heredada o reutilización de equipos SOHO en ambientes corporativos. La disponibilidad pública del exploit desde 2018 facilita que actores maliciosos automaticen campañas masivas de explotación sobre dispositivos expuestos a Internet.

- **Impacto:** Una explotación exitosa podría permitir el secuestro remoto del router, modificación de configuraciones críticas, incorporación del dispositivo a botnets maliciosos, exposición de tráfico institucional, persistencia remota y compromiso de conectividad organizacional, afectando directamente la seguridad de la infraestructura perimetral institucional.

Riesgos asociados a dispositivos End-of-Life (EoL)

- **Descripción:** Muchos routers ASUS afectados corresponden a dispositivos que ya no reciben actualizaciones oficiales de seguridad o presentan soporte limitado por parte del fabricante. En numerosos entornos organizacionales y del sector salud, este tipo de equipos continúa siendo utilizado para soportar redes inalámbricas, sedes remotas, servicios de telemedicina, conectividad administrativa, enlaces VPN y acceso a plataformas cloud. La permanencia de dispositivos EoL incrementa considerablemente el riesgo de explotación sostenida debido a ausencia de parches, vulnerabilidades conocidas acumuladas y limitaciones de monitoreo sobre infraestructura heredada.
- **Impacto:** Los atacantes podrían mantener persistencia prolongada dentro de la infraestructura comprometida, reutilizar exploits públicos ampliamente conocidos, comprometer tráfico institucional, desarrollar movimiento lateral y utilizar la infraestructura afectada para operaciones maliciosas posteriores, incrementando progresivamente el riesgo organizacional.

CSIRTSALUD-AL-20260525-105

TLP: CLEAR

Exposición sobre servicios administrativos y acceso remoto

- **Descripción:** Uno de los principales riesgos identificados corresponde a la exposición de servicios administrativos accesibles desde Internet. Muchos routers vulnerables mantienen habilitados paneles administrativos remotos, servicios de gestión, puertos expuestos, acceso WAN y configuraciones inseguras o por defecto. La explotación de CVE-2018-5999 permite que actores maliciosos interactúen con determinados mecanismos administrativos sin requerir autenticación válida, facilitando el control indebido del dispositivo.

- **Impacto:** Una explotación exitosa podría permitir modificación de credenciales administrativas, habilitación de accesos ocultos, alteración de configuraciones DNS, manipulación de tráfico institucional, espionaje de comunicaciones y control remoto persistente del dispositivo comprometido, facilitando posteriores actividades maliciosas dentro de la red organizacional.

Riesgos asociados a botnets sobre infraestructura IoT

- **Descripción:** El botnet RondoDox evidencia el crecimiento de amenazas dirigidas contra dispositivos IoT e infraestructura perimetral vulnerable. Los atacantes utilizan automatización masiva para identificar dispositivos vulnerables, explotar routers expuestos, incorporar equipos a botnets distribuidos y desarrollar campañas coordinadas de explotación. Los dispositivos comprometidos suelen operar continuamente y permanecer conectados a Internet durante largos periodos, lo que incrementa significativamente su valor operacional para actores maliciosos.

- **Impacto:** Los equipos afectados podrían ser utilizados para ataques DDoS distribuidos, campañas coordinadas, ocultamiento de tráfico malicioso, distribución de malware, relay de comunicaciones y afectación reputacional institucional. Asimismo, la infraestructura

comprometida podría participar involuntariamente en operaciones criminales dirigidas contra terceros objetivos.

Exposición sobre redes institucionales y servicios clínicos

- **Descripción:** En el sector salud, los routers vulnerables representan un punto crítico de exposición debido a la creciente dependencia sobre conectividad IP y servicios distribuidos. Muchos entornos hospitalarios soportan operaciones críticas mediante plataformas clínicas, sistemas HIS, telemedicina, aplicaciones interoperables, servicios cloud híbridos, autenticación remota y redes inalámbricas institucionales. El compromiso de dispositivos perimetrales podría facilitar acceso indirecto hacia servicios internos y componentes críticos organizacionales.

- **Impacto:** Una explotación exitosa podría generar interrupción de conectividad, degradación operacional, afectación sobre servicios médicos, indisponibilidad institucional, pérdida de integridad de comunicaciones y afectación de continuidad del negocio, impactando directamente procesos clínicos y administrativos críticos.

Riesgos asociados a segmentación insuficiente de red

- **Descripción:** Muchas organizaciones mantienen infraestructura perimetral conectada directamente con redes corporativas internas sin controles adecuados de segmentación. En escenarios vulnerables, un atacante que comprometa un router podría intentar desarrollar movimiento lateral, identificar dispositivos internos, comprometer servicios adicionales, inspeccionar tráfico sensible y acceder a segmentos críticos de la infraestructura organizacional. La ausencia de segmentación adecuada incrementa considerablemente el impacto potencial de este tipo de amenazas.

- **Impacto:** Los atacantes podrían expandir progresivamente el compromiso dentro de la red institucional, afectar múltiples servicios simultáneamente, comprometer dispositivos IoT, interceptar comunicaciones internas y aumentar significativamente la superficie de ataque organizacional.

Riesgos asociados a monitoreo insuficiente sobre infraestructura de borde

- **Descripción:** Muchos entornos organizacionales carecen de mecanismos adecuados de monitoreo y supervisión sobre routers y dispositivos perimetrales. En numerosos escenarios, los dispositivos comprometidos continúan operando aparentemente de forma normal, dificultando la detección temprana del incidente. Los atacantes podrían aprovechar esta situación para mantener persistencia prolongada, ocultar actividad maliciosa y desarrollar campañas automatizadas sin ser detectados oportunamente.

- **Impacto:** La falta de monitoreo podría facilitar compromiso prolongado, detección tardía, incremento del impacto operacional, abuso continuo de infraestructura institucional y escalamiento progresivo del incidente de seguridad, afectando significativamente la capacidad de respuesta organizacional.

Recomendaciones

Se recomienda a las organizaciones del sector salud implementar de manera prioritaria medidas orientadas a fortalecer la seguridad de la infraestructura perimetral, reducir la exposición de dispositivos vulnerables y minimizar el riesgo de compromiso asociado a campañas automatizadas dirigidas contra routers ASUS y dispositivos IoT conectados.

Gestión y actualización de dispositivos vulnerables

Las entidades deben realizar un inventario completo de routers ASUS y demás dispositivos perimetrales conectados a la infraestructura institucional, identificando versiones de firmware, estado de soporte y nivel de exposición hacia Internet. Es fundamental validar si los dispositivos afectados continúan operando con versiones vulnerables asociadas a CVE-2018-5999 o corresponden a equipos End-of-Life sin soporte vigente por parte del fabricante.

Se recomienda aplicar inmediatamente las actualizaciones de firmware disponibles y establecer procedimientos formales de gestión de vulnerabilidades sobre infraestructura de red. En escenarios donde los dispositivos ya no reciban soporte oficial, debe evaluarse prioritariamente su reemplazo por soluciones modernas que mantengan actualizaciones activas de seguridad.

Asimismo, las organizaciones deberían implementar políticas periódicas de revisión y actualización sobre:

- routers institucionales;
- firewalls perimetrales;
- puntos de acceso inalámbrico;
- dispositivos IoT;
- controladores de red;
- y equipos de conectividad remota.

Restricción de exposición hacia Internet

Las organizaciones deben reducir al mínimo la exposición directa de dispositivos administrativos hacia Internet. Se recomienda deshabilitar cualquier servicio de administración remota que no sea estrictamente necesario, incluyendo:

- acceso WAN administrativo;
- servicios Telnet;
- UPnP innecesario;
- puertos administrativos expuestos;
- servicios HTTP inseguros;
- y mecanismos heredados de administración remota.

Cuando el acceso remoto sea requerido por necesidades operacionales, se recomienda implementar controles adicionales como:

- VPN institucional;
- listas blancas de direcciones IP;
- autenticación multifactor;
- segmentación administrativa;
- cifrado robusto;
- y monitoreo continuo de accesos.

También se recomienda restringir el acceso administrativo únicamente desde redes internas seguras y evitar la administración directa desde Internet pública.

Fortalecimiento de configuraciones de seguridad

Es importante revisar y endurecer las configuraciones de seguridad presentes en routers y dispositivos perimetrales. Muchas campañas automatizadas aprovechan configuraciones inseguras, credenciales débiles o servicios habilitados por defecto.

Se recomienda:

- modificar inmediatamente credenciales predeterminadas;
- utilizar contraseñas robustas y únicas;
- deshabilitar cuentas innecesarias;
- eliminar servicios no utilizados;

- restringir permisos administrativos;
- y desactivar funcionalidades inseguras habilitadas por defecto.

Adicionalmente, se recomienda validar periódicamente:

- configuraciones DNS;
- reglas NAT;
- redireccionamientos;
- configuraciones VPN;
- usuarios administrativos;
- certificados instalados;
- y reglas de acceso remoto.

Cualquier cambio no autorizado debe ser tratado como posible indicador de compromiso.

Segmentación y aislamiento de infraestructura crítica

Las organizaciones del sector salud deben fortalecer la segmentación de red para evitar que un compromiso sobre dispositivos perimetrales facilite movimiento lateral hacia servicios críticos institucionales.

Se recomienda aislar adecuadamente:

- plataformas clínicas;
- sistemas HIS;
- dispositivos médicos;
- redes administrativas;
- servicios IoT;
- infraestructura cloud;
- redes de invitados;
- y entornos de telemedicina.

Los dispositivos perimetrales no deben poseer acceso innecesario hacia segmentos críticos internos. Asimismo, deben implementarse controles de filtrado, listas ACL, microsegmentación y políticas Zero Trust que limiten la capacidad de propagación dentro de la infraestructura.

En entornos hospitalarios, esta medida resulta especialmente importante debido a la coexistencia de:

- dispositivos biomédicos;
- aplicaciones clínicas;
- redes inalámbricas;
- sistemas administrativos;
- y servicios interoperables críticos.

Monitoreo y detección temprana

Se recomienda fortalecer las capacidades de monitoreo sobre infraestructura de borde y dispositivos IoT institucionales.

Las organizaciones deberían supervisar continuamente:

- cambios administrativos sobre routers;
- modificaciones DNS;
- reinicios inesperados;
- incremento anómalo de tráfico;
- conexiones salientes sospechosas;
- intentos de autenticación fallidos;
- y comportamiento inusual de dispositivos perimetrales.

Asimismo, se recomienda integrar eventos provenientes de routers y dispositivos de red dentro de plataformas SIEM institucionales para facilitar:

- correlación de eventos;
- detección de anomalías;

- identificación de actividad botnet;
- y respuesta temprana ante incidentes.

Es importante establecer alertas relacionadas con:

- cambios de configuración;
- habilitación de acceso remoto;
- alteraciones de firmware;
- actividad DDoS;
- y creación de cuentas administrativas inesperadas.

Protección frente a botnets y amenazas IoT

Debido al crecimiento de campañas automatizadas orientadas a dispositivos IoT y routers vulnerables, las organizaciones deben fortalecer controles específicos sobre este tipo de infraestructura.

Se recomienda implementar:

- filtrado de tráfico saliente;
- limitación de conexiones sospechosas;
- inspección de comportamiento anómalo;
- segmentación de dispositivos IoT;
- listas de reputación;
- y controles anti-DDoS.

Las entidades también deberían realizar evaluaciones periódicas orientadas a identificar:

- dispositivos expuestos;
- servicios innecesarios;
- configuraciones inseguras;

- firmware vulnerable;
- y actividad asociada a infraestructura botnet.

En entornos clínicos, es especialmente importante monitorear dispositivos médicos conectados y validar que no compartan segmentos inseguros con infraestructura administrativa o dispositivos vulnerables.

Gestión de incidentes y continuidad operacional

Las organizaciones deben preparar procedimientos específicos de respuesta ante incidentes relacionados con compromiso de infraestructura perimetral y dispositivos IoT.

Se recomienda establecer capacidades para:

- aislamiento rápido de dispositivos comprometidos;
- reemplazo controlado de routers afectados;
- restauración segura de configuraciones;
- recuperación operacional;
- análisis forense;
- y validación de integridad de configuraciones.

Asimismo, las entidades deberían mantener respaldos seguros y actualizados de:

- configuraciones de routers;
- políticas de red;
- configuraciones VPN;
- reglas de seguridad;
- y parámetros críticos de conectividad.

En el sector salud, estas medidas son fundamentales para reducir el impacto potencial sobre:

- continuidad clínica;
- disponibilidad de plataformas médicas;
- conectividad hospitalaria;
- servicios interoperables;
- y operación institucional crítica.

Sensibilización y fortalecimiento organizacional

Finalmente, se recomienda fortalecer la cultura de seguridad sobre infraestructura de red y dispositivos conectados.

Los equipos técnicos y administrativos deben recibir capacitación relacionada con:

- riesgos asociados a dispositivos IoT;
- explotación de routers vulnerables;
- campañas botnet;
- buenas prácticas de hardening;
- monitoreo de infraestructura perimetral;
- y respuesta ante incidentes de conectividad.

Asimismo, las organizaciones deberían incorporar evaluaciones periódicas de seguridad sobre infraestructura perimetral dentro de sus programas de gestión de riesgos y ciberseguridad institucional.

Conclusiones

La campaña asociada al botnet RondoDox evidencia cómo vulnerabilidades antiguas, ampliamente conocidas y con exploits públicos continúan representando un riesgo significativo para organizaciones que mantienen infraestructura perimetral desactualizada o insuficientemente protegida.

CSIRTSALUD-AL-20260525-105 **TLP: CLEAR**

La explotación activa de la vulnerabilidad CVE-2018-5999 demuestra que los actores maliciosos continúan aprovechando dispositivos vulnerables expuestos a Internet para desarrollar operaciones automatizadas orientadas a:

- conformación de botnets;
- ataques DDoS;
- espionaje de tráfico;
- persistencia remota;
- y expansión de infraestructura criminal distribuida.

Este escenario refleja el incremento progresivo de amenazas dirigidas contra dispositivos IoT, routers y componentes de conectividad que históricamente han recibido menor atención en comparación con servidores, estaciones de trabajo o plataformas cloud tradicionales.

En el contexto del sector salud, la situación adquiere una relevancia crítica debido a la creciente dependencia tecnológica sobre:

- redes hospitalarias distribuidas;
- plataformas clínicas interoperables;
- servicios de telemedicina;
- infraestructura cloud híbrida;
- dispositivos médicos conectados;
- y servicios digitales soportados sobre conectividad IP.

El compromiso de infraestructura perimetral podría facilitar afectaciones significativas sobre la confidencialidad, integridad y disponibilidad de servicios clínicos y administrativos críticos, impactando directamente la continuidad operacional institucional.

La amenaza también evidencia cómo los dispositivos de borde pueden convertirse en vectores estratégicos para desarrollar:

- movimiento lateral;
- persistencia prolongada;

- manipulación de tráfico;
- ataques encadenados;
- y compromisos progresivos sobre infraestructura organizacional.

Uno de los principales factores de riesgo identificados corresponde al uso continuo de dispositivos End-of-Life o firmware desactualizado, así como la exposición innecesaria de servicios administrativos hacia Internet pública. La ausencia de segmentación adecuada, monitoreo limitado y controles insuficientes sobre infraestructura IoT incrementa considerablemente la superficie de ataque disponible para actores maliciosos.

Las organizaciones del sector salud deben fortalecer prioritariamente sus capacidades de:

- gestión de vulnerabilidades;
- actualización de firmware;
- segmentación de red;
- monitoreo de infraestructura perimetral;
- protección de dispositivos IoT;
- y respuesta ante incidentes asociados a conectividad y dispositivos de borde.

Asimismo, resulta fundamental adoptar enfoques preventivos orientados a Zero Trust, hardening de infraestructura, reducción de exposición externa y supervisión continua de dispositivos críticos conectados a la red institucional.

Finalmente, este incidente demuestra que las amenazas modernas ya no se limitan únicamente a servidores o estaciones de trabajo tradicionales, sino que abarcan de manera creciente routers, dispositivos IoT, infraestructura cloud, plataformas de conectividad y componentes automatizados que forman parte esencial de los ecosistemas digitales modernos del sector salud.

Fuentes:

- https://hackread.com/rondodox-botnet-2018-vulnerability-hijack-asus-routers/?utm_source=chatgpt.com
- https://www.bankinfosecurity.com/rondodox-botnet-exploits-2018-flaw-in-asus-routers-a-31768?utm_source=chatgpt.com
- https://www.fing.com/news/new-asus-router-vulnerability-attack/?utm_source=chatgpt.com
- https://nvd.nist.gov/vuln/detail/CVE-2018-5999?utm_source=chatgpt.com
- https://www.cve.org/CVERecord?id=CVE-2018-5999
- https://www.asus.com/security-advisory/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.