NAME:WRECK
Vulnerabilidades DNS en pilas TCP/IP

BCSC- VULNERABILIDADES-NAME:WRECK

TLP:WHITE

www.basquecybersecurity.eus

Abril 2021

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

Investigadores de la compañía Forescout Research Labs, en asociación con el grupo de investigación de seguridad con sede en Israel JSOF Research, han revelado un conjunto de vulnerabilidades que afectan a 4 populares pilas TCP/IP. Estas vulnerabilidades a las que han nombrado NAME:WREC, se centran en el sistema de nombres de dominio (DNS) y pueden causar una denegación de servicio (DoS) o la ejecución remota de código (RCE), lo que permite a los atacantes obtener el control sobre los dispositivos afectados.

Los fallos se han encontrado en pilas TCP/IP que se ejecutan en una amplia gama de productos, desde servidores de alto rendimiento y equipos de red hasta sistemas de tecnología operativa (OT) que monitorizan y controlan equipos industriales. Por lo tanto, el uso generalizado de estas pilas y, a menudo, la exposición externa de clientes DNS vulnerables indican una superficie de ataque muy amplia. Todos estos fallos reportados se suman a vulnerabilidades similares descubiertas en investigaciones anteriores (Ripple20 y AMNESIA:33) que también afectaban a los servidores DNS.

Las vulnerabilidades descubiertas afectan a Nucleus NET, FreeBSD y NetX. Nucleus NET se ha utilizado durante décadas en varios dispositivos críticos de IoT. FreeBSD, además de ser implementado en proyectos de código abierto, es ampliamente conocido por ser utilizado en servidores de alto rendimiento en millones de redes informáticas, incluidos importantes sitios web como Netflix. NetX se utiliza en ThreadX RTOS, un sistema operativo en tiempo real utilizado en millones de sistemas, como dispositivos médicos o impresoras.

Sin embargo, no todos los dispositivos que ejecutan Nucleus NET o FreeBSD son vulnerables a este tipo de fallos, pero si asumimos que el 1% de los más de 10.000 millones de dispositivos son vulnerables, podemos estimar que al menos 100 millones de dispositivos están afectados por estas vulnerabilidades englobadas bajo el nombre de NAME:WRECK.

En la investigación llevada a cabo se han podido identificar las versiones afectadas por estas vulnerabilidades:

- FreeBSD (versión 12.1): uno de los sistemas operativos más populares de la familia BSD.
- IPnet (versión VxWorks 6.6): desarrollado inicialmente por Interpeak, ahora está bajo mantenimiento de WindRiver y utilizado por el sistema operativo en tiempo real (RTOS) de VxWorks.
- NetX (versión 6.0.1): proyecto de código abierto mantenido por Microsoft bajo el nombre Azure RTOS NetX.
- Nucleus NET (versión 4.3): parte del Nucleus RTOS mantenido por Mentor Graphics (Siemens), utilizado en dispositivos médicos, industriales aeroespacial e IoT.

Según Forescout, una explotación exitosa de estas vulnerabilidades podría causar daños significativos a servidores gubernamentales o empresariales, instalaciones de atención médica o empresas en el negocio de fabricación. Estas vulnerabilidades permiten robar datos confidenciales o modificar y desconectar equipos para fines de sabotaje.

Las mitigaciones recomendadas para NAME:WRECK incluyen la limitación de la exposición de los dispositivos vulnerables críticos, utilización de servidores DNS internos y actualización de los dispositivos.

2. ANÁLISIS TÉCNICO

Los investigadores que han reportado estos fallos han podido detectar hasta nueve vulnerabilidades en total. Estos fallos permiten la ejecución de código de forma remota (RCE), ataques de denegación de servicio (DoS) o el envenenamiento de caché DNS. A continuación, se muestra un resumen de las nueve vulnerabilidades reportadas:

- CVE-2020-7461: Aprovecha un error de límite al analizar datos de paquetes DHCP en dhclient. Un atacante remoto desde la red local, puede enviar datos especialmente diseñados al cliente DHCP, desencadenar un desbordamiento de búfer y ejecutar código arbitrario en el sistema de destino.

- CVE-2016-20009: Aprovecha un error en la función de descompresión de mensajes que puede desembocar en un desbordamiento de pila que podría provocar la ejecución remota de código. Es un fallo previamente reportado por Exodus Intelligence y corregido por Wind River en 2016 al que nunca se le asignó un CVE hasta que ha sido solicitado este año.

- CVE-2020-15795: La función de análisis de etiquetas DNS no valida correctamente los nombres de las respuestas DNS. Un atacante con una posición privilegiada en la red podría utilizar esta vulnerabilidad para ejecutar código de forma remota.

- CVE-2020-27009: Permite al atacante enviar un paquete de respuesta DNS con una combinación de punteros de compresión inválidos que le autoriza para escribir datos arbitrarios en partes sensibles de la memoria de un dispositivo, pudiendo ejecutar código de forma remota

- CVE-2020-27736: Se sirve de un error en la funcionalidad de análisis de etiquetas de nombres de dominio DNS al no validar correctamente el nombre en las respuestas DNS. Estas respuestas mal formadas podrían resultar en una lectura fuera de límites y producir una denegación de servicio (DoS).

- CVE-2020-27737: Aprovecha un error en la validación de las longitudes y recuentos de los registros. Este fallo podría dar lugar a una lectura fuera de límites y permitir a un atacante causar una denegación de servicio (DoS).

- CVE-2020-27738: La función de descompresión de nombres DNS no valida correctamente los valores de desplazamiento del puntero. Estas respuestas mal formadas podrían resultar en una lectura fuera de límites, que podrían dar lugar a que un atacante provocara una denegación de servicio (DoS).

- CVE-2021-25677: El cliente DNS al no aleatoriza correctamente el ID de transacción de DNS y los números de puerto UDP, permitiendo a los atacantes realizar ataques de envenenamiento de caché DNS.

- Se ha reportado otra vulnerabilidad a la que todavía no se le ha asignado CVE y que afecta a las funciones *_nx_dns_name_string_unencode* y *_nx_dns_resource_name_real_size_calculate*. Al no verificar que el puntero de compresión no sea igual al mismo desplazamiento que se está analizando actualmente, podría llevar a un bucle infinito y puede provocar una denegación de servicio (DoS).

A continuación, se muestra una tabla resumen en la que se indica la tecnología afectada, el tipo de vulnerabilidad y la puntuación recibida acorde con la escala CVSSv3.

CVE	Tecnología afectada	Tipo vulnerabilidad	Puntuación
CVE-2020-7461	FreeBSD	RCE	7.7
CVE-2016-20009	IPnet	RCE	9.8
CVE-2020-15795	Nucleus NET	RCE	8.1
CVE-2020-27009	Nucleus NET	RCE	8.1
CVE-2020-27736	Nucleus NET	DoS	6.5
CVE-2020-27737	Nucleus NET	DoS	6.5
CVE-2020-27738	Nucleus NET	DoS	6.5
CVE-2021-25677	Nucleus NET	Spoofing	5.3
*	NetX	DoS	6.5

Las vulnerabilidades descritas anteriormente pueden exponer a ataques tanto a los dispositivos conectados a Internet como a los internos. A continuación, se muestra un escenario de ataque que aprovecha las vulnerabilidades de NAME:WRECK en objetivos internos y externos.

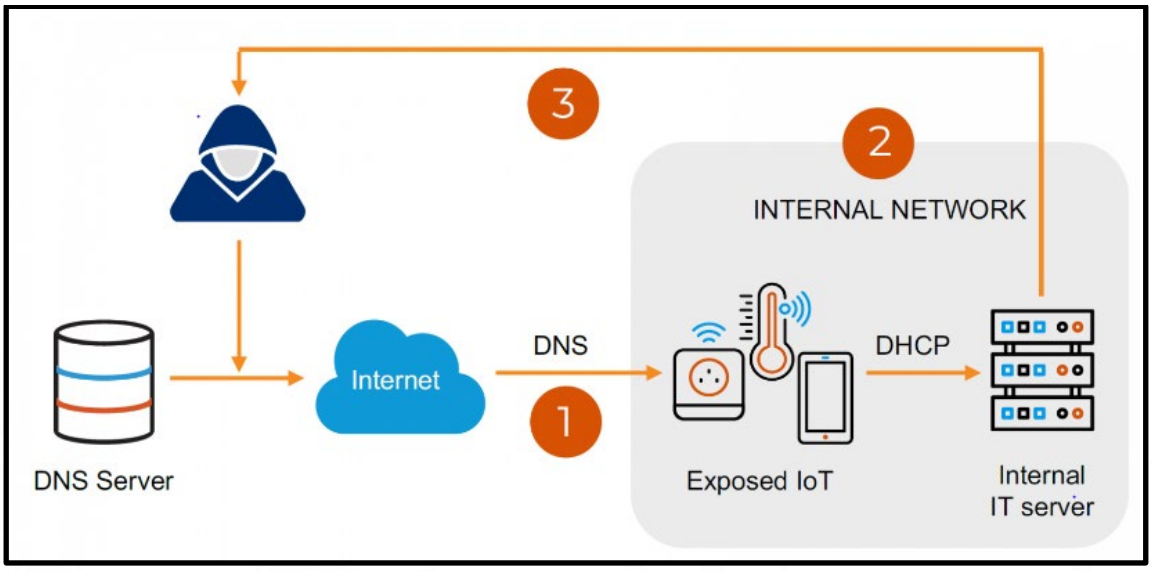

Figura 1: Escenario de ataque. Fuente Forescout.

El escenario que se propone se basa en ataques reales que han sucedido en el pasado y que han visto cómo los dispositivos IoT son utilizados como puntos de entrada. De hecho, se conocen ataques que incluyen la exfiltración de datos de la NASA utilizando una Raspberry Pi o el ataque a un casino de Las Vegas haciendo uso de un termómetro conectado a Internet como punto de entrada.

En el ejemplo propuesto, el atacante obtiene acceso inicial a una red de la organización (paso 1) comprometiendo un dispositivo que emite peticiones DNS a un servidor en Internet. Para obtener este acceso inicial el atacante puede explotar uno de los RCEs que afectan a Nucleus NET expuestos anteriormente.

Tras el acceso inicial, el atacante puede utilizar el punto de entrada comprometido para configurar un servidor DHCP interno y ejecutar código malicioso (paso 2) en servidores internos vulnerables que emitan peticiones DHCP.

Finalmente, el atacante puede utilizar esos servidores internos comprometidos para filtrar datos (paso 3) o hacerse con el control del dispositivo.

En cuanto a los recursos afectados por estas vulnerabilidades, los sistemas que utilizan las pilas TCP/IP afectadas son los siguientes:

- FreeBSD versión 12.1
- IPnet versión VxWorks 6.6
- NetX versión 6.0.1
- Nucleus NET versión 4.3

De todas formas, no todos los dispositivos que utilizan estos sistemas son vulnerables, pero se estima que al menos 100 millones de dispositivos son vulnerables a estos errores. Como dato, hay más de 1 millón de instancias de FreeBSD conectadas a Internet y más de 1.300 ejecutando Nucleus RTOS, siendo los sectores sanitario y gubernamental los más afectados:

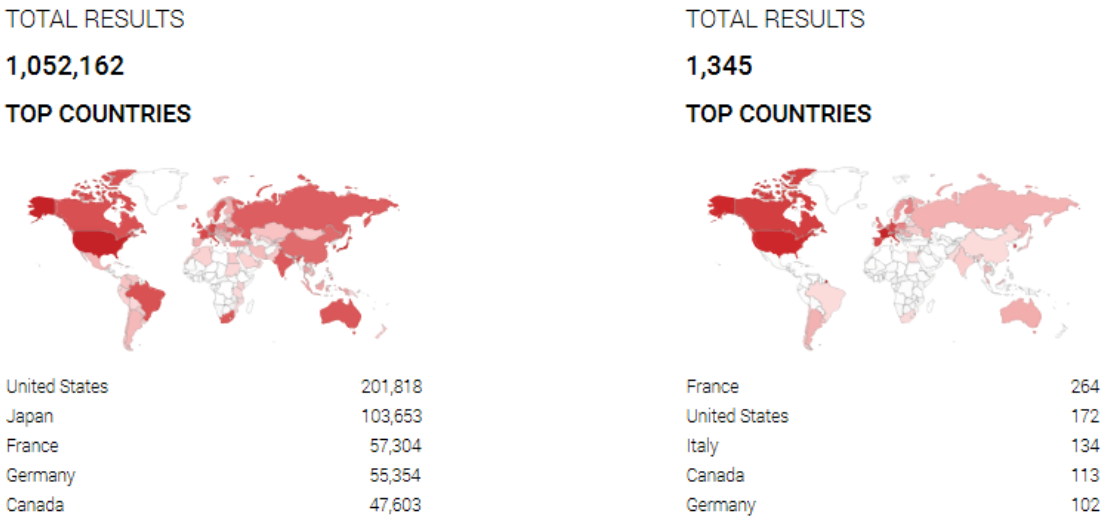

Figura 2: Sistemas FreeBSD y Nucleus RTOS expuestos en Internet.
Fuente Forescout.

3. MITIGACIÓN / SOLUCIÓN

La protección completa contra NAME:WRECK requiere parchear los dispositivos que ejecutan las versiones vulnerables de las pilas TCP/IP. FreeBSD, Nucleus NET y NetX han sido parcheados recientemente, y los proveedores de dispositivos que utilizan este software deberían proporcionar sus propias actualizaciones a los clientes. Por lo que es necesario parchear los dispositivos siguiendo estos pasos:

- Identificar qué sistema operativo se está ejecutando en sus dispositivos.
- Obtener las versiones de los paquetes actualmente instalados.
- Actualizar los sistemas vulnerables.

Estas operaciones pueden incluso automatizarse en caso de que los servidores soporten la gestión remota, vía SSH, por ejemplo. Por lo general, estos servidores están desplegados con alta disponibilidad y balanceo de carga, lo que significa que pueden ser reiniciados sin mayores problemas mientras otros servidores prestan un servicio similar.

En caso de no poder aplicar las actualizaciones indicadas por cada proveedor se recomiendan varias estrategias de mitigación:

- Realizar un inventario de los dispositivos que ejecutan las pilas vulnerables. Forescout Research Labs ha publicado un script de código abierto para detectar los dispositivos que ejecutan las pilas afectadas.
- Restringir las vías de comunicación externas y aislar o contener los dispositivos vulnerables.
- Configurar los dispositivos para que dependan de servidores DNS internos y vigilar de cerca el tráfico DNS externo, ya que la explotación de estas vulnerabilidades requiere de un servidor DNS externo para responder con paquetes maliciosos.
- Supervisar todo el tráfico de red en busca de paquetes maliciosos que intenten explotar vulnerabilidades conocidas o posibles vulnerabilidades de tipo zero-day. El tráfico anómalo debe ser bloqueado, o al menos, alertar de su presencia a los operadores de la red.

4. REFERENCIAS ADICIONALES

- Forescout: The impact of NAME:WRECK
- NAME:WRECK DNS vulnerabilities affect over 100 million devices.
- Millions of devices at risk from NAME:WRECK DNS bugs.
- These new vulnerabilities put millions of IoT devices at risk, so patch now.

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?