Vulnerabilidades Nimbuspwn

BCSC-VULNERABILIDADES- NIMBUSPWN

TLP:WHITE

www.basquecybersecurity.eus

Abril 2022

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

Los investigadores de seguridad de Microsoft, han descubierto dos vulnerabilidades críticas que afectan a sistemas Linux, y que han sido identificadas con el nombre de **Nimbuspwn.**

Estas vulnerabilidades, registradas con identificadores CVE-2022-29799 y CVE-2022-29800, se pueden encadenar para obtener privilegios de administrador en los sistemas Linux, lo que permitiría a los atacantes ejecutar malware así como realizar otras acciones maliciosas mediante la ejecución arbitraria de código root. Así mismo, las vulnerabilidades de **Nimbuspwn** podrían ser utilizadas por parte de amenazas más sofisticadas, como un vector de ataque para lograr un acceso efectivo al root e incrementar el potencial impacto del malware o ransomware en los dispositivos vulnerables.

Se recomienda a los usuarios de networkd-dispatcher que actualicen sus programas. Estas vulnerabilidades se solucionaron con el lanzamiento de **networkd-dispatcher 2.2**, aunque no hay información sobre la publicación de actualizaciones por distribuciones.

2. ANÁLISIS TÉCNICO

Investigadores de la compañía Microsoft descubrieron este conjunto de vulnerabilidades catalogadas bajo el nombre de **Nimbuspwn** tras realizar revisiones de código y análisis dinámicos en servicios que se ejecutan como root, identificando un patrón extraño en una unidad *systemd* llamada networkd-dispatcher.

Estas revisiones y análisis dinámicos revelaron múltiples problemas de seguridad, como, por ejemplo, cruce de directorios o condiciones de carrera, que pueden ser aprovechados para elevar privilegios dentro del sistema vulnerable e implementar malware, cargas útiles, como una puerta trasera, o realizar otras acciones maliciosas a través de la ejecución arbitraria de código con privilegios de root.

Las vulnerabilidades reportadas aprovechan el D-Bus, software que permite que los procesos en el mismo punto final se comuniquen transmitiendo mensajes y respondiendo a ellos. Destacar que existen muchos componentes de D-Bus de forma predeterminada en los entornos de escritorio Linux más populares. Dado que esos componentes se ejecutan con diferentes privilegios, son un objetivo atractivo para los atacantes, ya que normalmente tendrá algún servicio que se ejecuta como root.

A continuación, se indican los detalles técnicos dados a conocer de cada una de las vulnerabilidades:

- CVE-2022-29799: esta vulnerabilidad aprovecha un error en *networkd-dispatcher*. Este proceso, diseñado para ejecutar sólo secuencias de comandos del controlador del sistema ubicadas en el directorio */etc/networkd-dispatcher* y no reemplazable por el usuario, se ejecuta como root y escucha eventos a través del D-Bus. Pero, debido a esta vulnerabilidad, es posible modificar la ruta del directorio indicado anteriormente y ejecutar scripts arbitrarios alojados en un directorio propio, permitiendo la ejecución de código con privilegios de root.

  En particular, al formar la ruta del archivo, se utilizaron los valores *OperationalState* y *AdministrationState,* transmitidos a través de D-Bus, en los que no se borraron los caracteres especiales. Por lo tanto, un atacante podría generar su propio estado con los caracteres «../» en el nombre y redirigir la llamada networkd-dispatcher a otro directorio de su propiedad.

- CVE-2022-29800: esta vulnerabilidad está relacionada con una condición de carrera. Entre la verificación de los parámetros del script (pertenecientes a root) y su ejecución, existe un breve período de tiempo, suficiente para reemplazar el archivo y omitir la verificación del script propiedad del usuario root. Además, *networkd-dispatcher* no verifica los enlaces simbólicos, incluso al ejecutar scripts a través de la llamada *subprocess.Popen*, lo que simplifica enormemente la organización del ataque.

Un posible flujo de ataque combinando las dos vulnerabilidades anteriores podría ser el siguiente:

- Se crea el directorio */tmp/nimbuspwn*.
- Se crea un enlace simbólico */tmp/nimbuspwn/poc.d* que apunta al directorio */sbin* que se usa para pasar una verificación de archivos ejecutables propiedad de root.
- Para los archivos ejecutables de */sbin*, los archivos con el mismo nombre se crean en el directorio */tmp/nimbuspwn*, por ejemplo, para el archivo */sbin/vgs*, se crea un archivo ejecutable */tmp/nimbuspwn/vgs*, propiedad de un usuario sin privilegios, en el que se incluye el código que el atacante quiere ejecutar.
- Se envía una señal D-Bus al proceso *networkd-dispatcher* con *OperationalState* establecido en *«../../../tmp/nimbuspwn/poc»* (CVE-2022-29799).

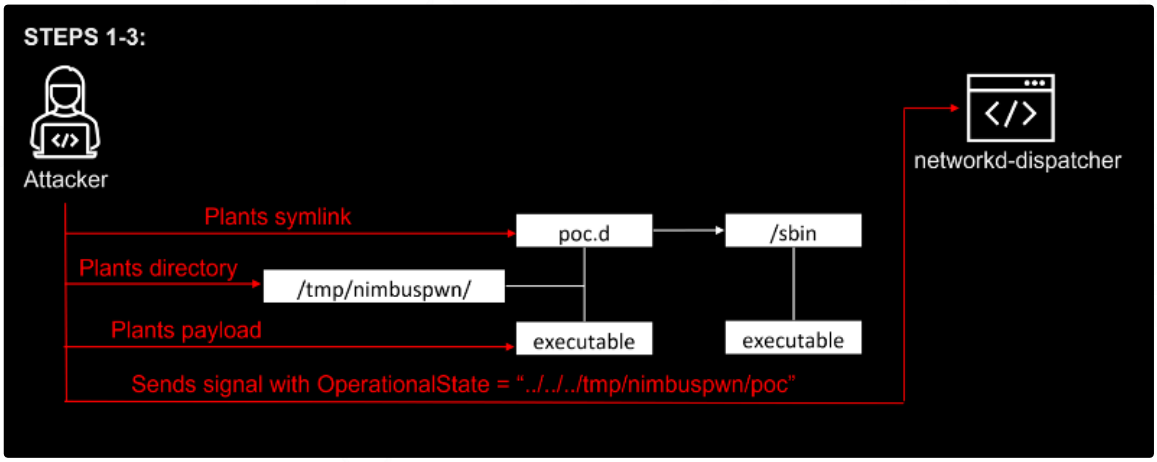

Imagen 1: Flujo de ataque. Pasos 1-3. Fuente: Microsoft 365 Defender.

- Al recibir la señal, n*etworkd-dispatcher* crea una lista de archivos ejecutables propiedad del usuario root y disponibles en el directorio */etc/networkd-dispatcher/../../../tmp/nimbuspwn/poc.d*, que en realidad se refiere a */sbin*.

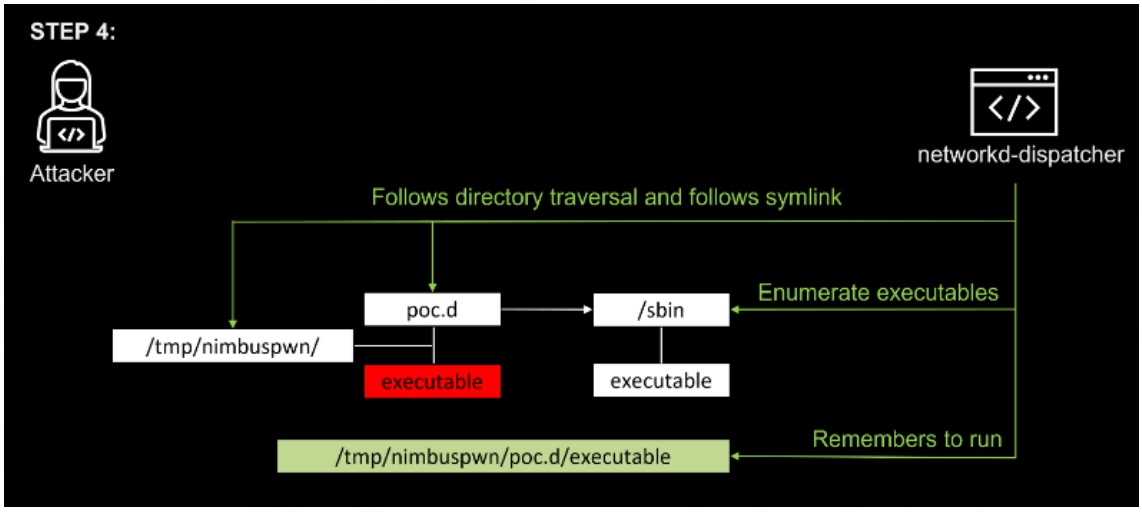

Imagen 2: Flujo de ataque. Paso 4. Fuente: Microsoft 365 Defender.

- En el momento en que se recibe la lista de archivos, pero aún no se ha ejecutado el script, el enlace simbólico se redirige de «/tmp/nimbuspwn/poc.d» a «/tmp/nimbuspwn» y networkd-dispatcher se ejecutará como root con el script inyectado por el atacante.

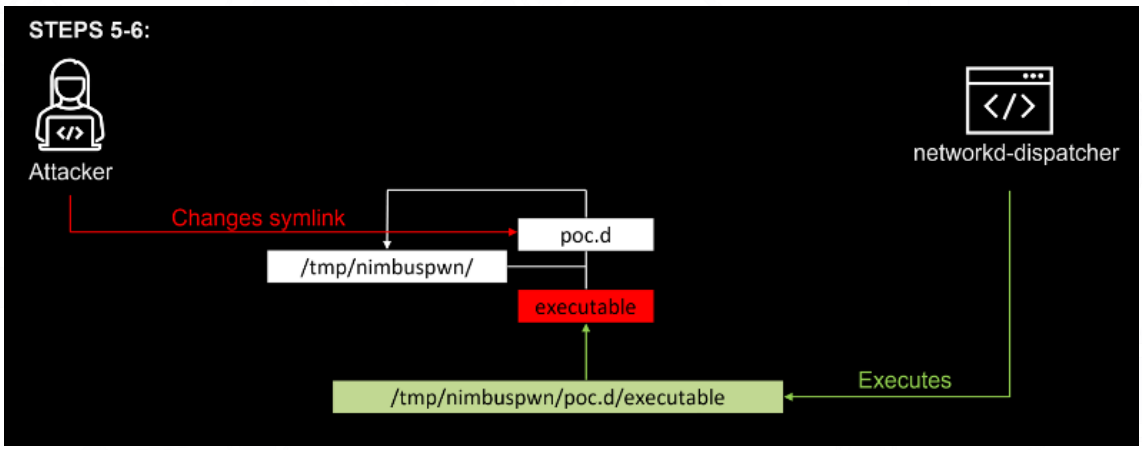

Imagen 3: Flujo de ataque. Paso 5. Fuente: Microsoft 365 Defender.

3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Se recomienda a los usuarios de networkd-dispatcher que actualicen sus instancias. Estas vulnerabilidades se solucionaron con el lanzamiento de **networkd-dispatcher 2.2**, aunque no hay información sobre la publicación de actualizaciones por distribuciones.

4. REFERENCIAS ADICIONALES

- Microsoft finds new elevation of privilege Linux vulnerability, Nimbuspwn.
- New Nimbuspwn Linux vulnerability gives hackers root privileges.
- Microsoft Discovers New Privilege Escalation Flaws in Linux System.
- Microsoft points at Linux and shouts.
- MITRE: CVE-2022-29799.
- MITRE: CVE-2022-29800.
- Linux Man Pages: networkd-dispatcher.
- Wikipedia: D-Bus.
- Wikipedia: systemd.
- Freedesktop.
- Inter Process Communication (IPC)
- Systemd.
- D-BUS – El sistema de comunicación de procesos para Desktop.

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?