Vulnerabilidad en Netmask (Node.js)

BCSC-Vulnerabilidad-Netmask-Node.js

TLP:WHITE

www.basquecybersecurity.eus

Abril 2021

TABLA DE CONTENIDO

Sobre el BCSC 3
Resumen ejecutivo 4
Análisis técnico 5
Mitigación / Solución 7
Referencias Adicionales 8

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:

RESUMEN EJECUTIVO

Los investigadores Victor Viale, Nick Sahler, Kelly Kaoudis, Sickcodes y John Jackson han descubierto una vulnerabilidad crítica en **Node.js,** entorno en tiempo de ejecución multiplataforma de código abierto basado en el lenguaje de programación JavaScript. Más concretamente el fallo reportado se localiza en el componente **netmask de la librería npm**. Este paquete alcanza más de **3 millones de descargas semanales** y se trata de un hallazgo especialmente importante debido a que este fallo ha estado presente durante más de 9 años.

A esta vulnerabilidad se le ha asignado el CVE-2021-28918 y se aprovecha de un error del componente netmask al procesar direcciones IPv4 decimales cuando contienen un cero a la izquierda.

Una explotación exitosa de dicha vulnerabilidad permite a atacantes remotos realizar ataques del tipo:

- **Server-side request forgery (SSRF):** ataques denominados de falsificación de solicitudes del lado del servidor. Un atacante puede forzar al servidor web a realizar peticiones desde dentro del sistema hacia el exterior con el fin de manipular información en el ámbito de ese servidor que de otro modo no sería directamente accesible.
- **Remote file inclusión (RFI):** vulnerabilidad existente solamente en páginas dinámicas en PHP que permite la inserción del enlace de archivos remotos situados en otros servidores a causa de una mala programación de la página.
- **Local file inclusión (LFI):** esta técnica consiste en incluir ficheros locales, es decir, archivos que se encuentran en el mismo servidor de la web, a diferencia de la vulnerabilidad RFI que incluye archivos alojados en otros servidores. En un escenario como este, un atacante podría modificar los parámetros e indicar al sitio web que se incluyan otros archivos que también están en el servidor, comprometiendo su seguridad por completo.

La explotación exitosa de esta vulnerabilidad puede permitir que un atacante remoto obtenga acceso a intranets o a equipos de la red LAN. Sin embargo, ya está disponible una actualización que soluciona estos fallos reportados y que se encuentra disponible siguiendo los pasos mostrados en el enlace indicado a continuación. Por lo tanto, se recomienda a todos los desarrolladores de node.js que usen el paquete *netmask* actualizar a la versión más reciente.

- https://www.npmjs.com/package/netmask

ANÁLISIS TÉCNICO

Una dirección IP se puede representar en una gran variedad de formatos, incluidos hexadecimal y entero, aunque las direcciones IPv4 más comunes se expresan en formato decimal. Por ejemplo, la dirección IPv4 del DNS de Google representada en formato decimal es 8.8.8.8, pero la misma se puede expresar en formato octal como 0010.0010.0010.0010.

La mayoría de las aplicaciones al recibir una dirección IPv4 en formato octal transforman automáticamente esta dirección a un formato decimal. Por ejemplo, si escribimos en cualquier navegador la dirección en octal 0127.0.0.1 el navegador modifica la dirección a su forma decimal.

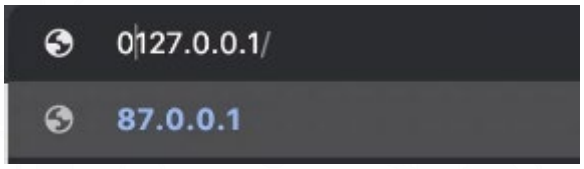

Imagen 1: Dirección octal transformada automáticamente en decimal por el navegador.

De acuerdo con la especificación original de IETF, partes de una dirección IPv4 se pueden interpretar como octal si tienen el prefijo "0". Sin embargo, la máscara de red ignora esto y siempre considera las partes como decimales, eliminando y descartando esos ceros. Esto significa que, en el caso expuesto anteriormente, los atacantes pueden forzar a un servidor a conectarse a la dirección 127.0.0.1 introduciendo realmente la dirección 0127.0.0.1.

A priori este error puede parecer poco importante, pero si un atacante modifica la entrada de la dirección IP que está siendo analizada por la aplicación, puede dar lugar a vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF).

Este error también se puede aprovechar para la inclusión remota y local de archivos. Un atacante puede crear una dirección IP que parezca privada para la máscara de red, debido a la forma en que la máscara de red convierte todas las partes de IPv4 (octetos) a formato decimal, pero en realidad la dirección IPv4 real es una dirección IP que apunta a otro servidor propiedad de los atacantes, en el que se alojan los archivos que se quieran incluir en el servidor legítimo.

Cualquier usuario aprovechando esta vulnerabilidad puede omitir paquetes que dependen de la máscara de red para filtrar bloques de direcciones IP y tener acceso a intranet, VPN, instancias de VPC o equipos de la red LAN, comprometiendo de esta forma la confidencialidad, disponibilidad e integridad del sistema. Esta vulnerabilidad afecta a todas las versiones de netmask npm en su versión 1.1.0 y anteriores.

Esta vulnerabilidad se ha catalogado como crítica, ya que permite modificar e insertar archivos en el servidor atacado de forma remota. Tiene una puntuación CVSS de 9.1.

Uno de los investigadores que ha participado en el análisis de esta vulnerabilidad ha publicado un repositorio en el que se puede obtener más información, así como una prueba de concepto en la que se pueden observar más detalles técnicos sobre este fallo:

- https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-011.md

MITIGACIÓN / SOLUCIÓN

Tras el informe de los investigadores detallando esta vulnerabilidad se ha parcheado el error en la versión 2.0.0. Esta actualización que soluciona estos fallos reportados se encuentra disponible, y se recomienda a todos los desarrolladores de node.js que usen el paquete netmask actualizar en cuanto sea posible:

- https://www.npmjs.com/package/netmask

Por otro lado, el desarrollador Olivier Poitrey ha publicado una serie de correcciones que validan que los octetos de IPv4 con prefijos 0 se tratan como octal y no como números decimales, solventando el error que daba lugar a las vulnerabilidades:

- https://github.com/rs/node-netmask/commit/4678fd840ad0b4730dbad2d415712c0782e886cc#diff-04f4f5b6e6cd99b4a664143f590d40d005f9b658d4ae0678ddc25c49bed19e2bR12-R17

REFERENCIAS ADICIONALES

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28918
- https://nvd.nist.gov/vuln/detail/CVE-2021-28918
- https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-011.md
- https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/
- https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/
- https://sick.codes/universal-netmask-npm-package-used-by-270000-projects-vulnerable-to-octal-input-data-server-side-request-forgery-remote-file-inclusion-local-file-inclusion-and-more-cve-2021-28918/

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?