Vulnerabilidades AMNESIA:33

BCSC_Alerta_Vulnerabilidades_AMNESIA:33

TLP:WHITE

www.basquecybersecurity.eus

Diciembre 2020

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 Repuesta 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

Investigadores de seguridad de la firma Forescout han alertado sobre múltiples vulnerabilidades en las pilas TCP/IP incorporadas en millones de dispositivos, desde equipos de red y dispositivos médicos hasta sistemas de control industrial, que podrían ser explotadas por atacantes para tomar el control de dichos sistemas. Denominados colectivamente como "**AMNESIA:33**", los fallos descubiertos son un conjunto de **33 vulnerabilidades** que afectan a cuatro pilas de protocolos TCP/IP de código abierto (uIP, FNET, picoTCP y NutNet) utilizados normalmente en **dispositivos IoT**. Como consecuencia de una gestión inadecuada de la memoria, una explotación satisfactoria de estos fallos podría causar una corrupción de memoria, permitiendo a los atacantes comprometer dichos dispositivos, ejecutar código malicioso, realizar ataques de denegación de servicio (DoS), robar información sensible e incluso envenenar la memoria caché del DNS. En un escenario real, la explotación de estas vulnerabilidades podría llegar a provocar interrupciones en el funcionamiento de una central eléctrica o la desconexión de sistemas de alarma de humo y de control de temperatura.

Se calcula que **millones de dispositivos de unos 158 fabricantes diferentes son vulnerables** a AMNESIA:33, afectando a múltiples pilas de TCP/IP de código abierto que no son propiedad de una sola compañía.

ANÁLISIS TÉCNICO

Las pilas TCP/IP integradas brindan una capacidad de comunicación de red esencial en redes TCP/IP para muchos sistemas operativos ligeros implementados en dispositivos IoT, dispositivos integrados y tecnologías como *Edge Computing*, es decir, computación perimetral.

Las pilas de TCP/IP son componentes críticos de todos los dispositivos conectados a una dirección IP, ya que permiten comunicaciones de red básicas.

Un fallo de seguridad en una pila TCP/IP puede ser extremadamente peligroso dado que el código de estos componentes puede usarse para procesar cada paquete de red entrante que llega a un dispositivo. Esto significa que ciertas vulnerabilidades en una pila de TCP/IP podrían permitir a un atacante comprometer por completo un dispositivo, incluso cuando simplemente se encuentra en una red sin ejecutar una aplicación específica.

Ilustración 1. Vulnerabilidades "AMNESIA:33"

En este sentido, **AMNESIA:33** es un conjunto de 33 vulnerabilidades descubiertas en los protocolos de cuatro pilas TCP/IP utilizadas por los principales proveedores de dispositivos de IoT, OT y TI: **uIP**, **FNET**, **picoTCP** y **NutNet**. La explotación de estas vulnerabilidades podría permitir a un atacante tomar el control de un dispositivo, usándolo como un punto de entrada en una red para dispositivos conectados a Internet, como un punto de pivote para el movimiento lateral, como un punto de persistencia en la red objetivo o como el punto final objetivo de un ataque. Para las organizaciones empresariales, esta circunstancia significa que el riesgo de que su red se vea comprometida, así como que los actores malintencionados socaven la continuidad de su negocio se ve notablemente incrementado. Para los usuarios particulares, esto significa que sus dispositivos IoT podrían ser usados como parte de grandes campañas de ataque, como botnets, sin que estos puedan percatarse.

A continuación, se citan las 3 vulnerabilidades más destacadas dentro de AMNESIA:33 y que han sido calificadas como críticas, junto a una breve descripción de cada una:

- **CVE-2020-24336**: El código para analizar los registros DNS en los paquetes de respuesta DNS enviados a través de NAT64 no valida el campo de longitud de los registros de respuesta, lo que permite a los atacantes dañar la memoria.
- **CVE-2020-24338**: La función que analiza los nombres de dominio carece de comprobaciones de límites, lo que permite a los atacantes dañar la memoria con paquetes DNS especialmente diseñados.
- **CVE-2020-25111**: Existe un desbordamiento de búfer en la pila que se produce durante el procesamiento del campo de nombre de un registro de recursos de respuesta de DNS, lo que permite a un atacante dañar la memoria adyacente escribiendo un número arbitrario de bytes en un búfer asignado.

El listado total de CVE asignados a las 33 vulnerabilidades, junto a su criticidad asignada por el **CISA ICS-CERT** en base a la escala **CVSSv3**, se puede consultar a través de la siguiente tabla:

CVE	Criticidad (CVSSv3)
CVE-2020-13984	7.5
CVE-2020-13985	7.5
CVE-2020-13986	7.5
CVE-2020-13987	8.2
CVE-2020-13988	7.5
CVE-2020-17437	8.2
CVE-2020-17438	7.0
CVE-2020-17439	8.1
CVE-2020-17440	7.5
CVE-2020-17441	7.5
CVE-2020-17442	7.5
CVE-2020-17443	8.2
CVE-2020-17444	7.5
CVE-2020-17445	7.5
CVE-2020-17467	8.2
CVE-2020-17468	7.5
CVE-2020-17469	5.9
CVE-2020-17470	4.0
CVE-2020-24334	8.2
CVE-2020-24335	7.5
CVE-2020-24336	**9.8**
CVE-2020-24337	7.5
CVE-2020-24338	**9.8**

CVE-2020-24339	7.5
CVE-2020-24340	8.2
CVE-2020-24341	8.2
CVE-2020-24383	6.5
CVE-2020-25107	7.5
CVE-2020-25108	7.5
CVE-2020-25109	8.2
CVE-2020-25110	8.2
CVE-2020-25111	**9.8**
CVE-2020-25112	8.1

Los investigadores responsables del estudio y reporte de estas vulnerabilidades han publicado un informe completo y video explicativo sobre los fallos:

- **Informe**:
  - https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/
- **Video**:
  - AMNESIA:33 - Forescout

Hasta la fecha, no se tiene conocimiento sobre la explotación activa de estas vulnerabilidades.

MITIGACIÓN / SOLUCIÓN

Algunos de los 150 fabricantes afectados ya han publicado sus correspondientes avisos de seguridad:

- Devolo
- EMU Electronic AG
- FEIG
- Genetec
- Harting
- Hensoldt
- Microchip
- Nanotec
- NT-Ware
- Tagmaster
- Siemens
- Uniflow
- Yanzi Networks

Debido a la complejidad de identificar y parchear dispositivos vulnerables, se recomienda adoptar soluciones que ofrezcan visibilidad granular de los dispositivos, permitan la monitorización de las comunicaciones de red y aíslen los dispositivos o segmentos de red vulnerables para administrar el riesgo que representan estas vulnerabilidades.

Además, se recomienda tomar medidas defensivas genéricas para minimizar el riesgo de explotación de estas vulnerabilidades:

- Minimizar la exposición en la red para todos los dispositivos y/o sistemas de control y asegurarse de que no sean accesibles desde Internet.
- Ubicar las redes de los sistemas de control y los dispositivos remotos detrás de firewalls y aislarlos de la red empresarial.
- Cuando se requiera acceso remoto, utilizar métodos seguros, como redes privadas virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más actual disponible.
- Utilizar un servidor DNS interno que realice DNS sobre HTTPS para las búsquedas.

REFERENCIAS ADICIONALES

- AMNESIA:33. How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices
- ICS Advisory (ICSA-20-343-01) - Multiple Embedded TCP/IP Stacks
- Embedded TCP/IP stacks have memory corruption vulnerabilities - Vulnerability Note VU#815128

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?