Número 96 | Noviembre 2024

NTT DATA

Radar

El magazine de ciberseguridad

Privacidad: ¿un derecho o un privilegio?

Por Francisco Javier García Lorente

La privacidad ha emergido como uno de los temas más polémicos y fundamentales de nuestra sociedad. A medida que la tecnología avanza a un ritmo impetuoso, la línea que separa la privacidad como un derecho esencial y su consideración como un privilegio exclusivo se vuelve cada vez más borrosa. Este debate tiene repercusiones legales, sociales y tecnológicas que afectan a cada persona. Por ello, debemos reflexionar, ¿es la privacidad un derecho inherente o un privilegio reservado para aquellos con los recursos necesarios para protegerla?

La privacidad como derecho humano fundamental

En muchos países, la privacidad es reconocida como un derecho fundamental. El artículo 12 de la Declaración Universal de los Derechos Humanos establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Este principio se ha expandido a través de diversas constituciones y legislaciones a lo largo del mundo.

Bajo este prisma, la privacidad no es solo el derecho a no ser observado o interferido sin consentimiento, sino también a tener control sobre la información personal, cómo se recopila, utiliza y comparte. Esta noción ha sido fortalecida por marcos regulatorios como el vigente Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que ofrece un enfoque robusto para garantizar que los ciudadanos tengan el control sobre sus datos.

Sin embargo, aunque la ley reconozca la privacidad como un derecho, la implementación y aplicación efectiva de este derecho varía considerablemente. No todos los ciudadanos, ni siquiera en países con regulaciones estrictas, disfrutan de la misma protección de su privacidad. Aquí es donde surge la cuestión de si la privacidad es un derecho igualitario o si, en la práctica, se convierte en un privilegio accesible solo para unos pocos.

La erosión de la privacidad en la era digital

El avance de la tecnología ha traído consigo una cantidad exponencial de nuevas herramientas y plataformas que, si bien hacen la vida más eficiente, también han socavado de manera significativa la privacidad. Redes sociales, aplicaciones móviles, dispositivos IoT, y algoritmos de inteligencia artificial recopilan enormes cantidades de datos sobre sus usuarios. Esta información no solo se utiliza para mejorar los servicios, sino también para fines comerciales y de vigilancia.

El problema radica en que, a menudo, las personas no son conscientes de la magnitud de los datos que se recogen o de las implicaciones que esto puede tener. Muchas veces, aceptan términos y condiciones sin leerlos, renunciando así al control de su información personal. Las grandes corporaciones tecnológicas, como Google, Facebook o Amazon, utilizan esta información para generar perfiles detallados de los usuarios, lo que genera preocupaciones sobre cómo se utiliza esta información, quién tiene acceso a ella, y con qué propósitos.

En este escenario, quienes tienen el poder financiero y tecnológico para proteger su privacidad —a través de medidas como el cifrado de comunicaciones, VPNs, o incluso mediante el pago de servicios premium sin publicidad— disfrutan de mayores niveles de privacidad que aquellos que no tienen acceso a estos recursos. Esto plantea la inquietante pregunta de si la privacidad se está convirtiendo en un privilegio reservado para las élites tecnológicas y económicas.

La desigualdad en la privacidad digital

La accesibilidad a herramientas de privacidad avanzadas crea una barrera entre los ciudadanos comunes y aquellos con más recursos. Las personas con altos conocimientos tecnológicos pueden configurar sus dispositivos y aplicaciones para minimizar la recolección de datos, pero para el ciudadano promedio, esta capacidad es limitada. Muchas veces, la privacidad se sacrifica a cambio de conveniencia o de acceso a servicios "gratuitos" que en realidad comercian con los datos personales como moneda de cambio.

Un claro ejemplo de esto son los motores de búsqueda y las redes sociales. Empresas como Google y Facebook ofrecen servicios gratuitos a los usuarios, pero monetizan estos servicios recopilando enormes cantidades de datos sobre su comportamiento en línea para vender publicidad dirigida.

Para evitar esto, un usuario puede optar por servicios de pago que prometen mayor protección de la privacidad, como motores de búsqueda sin rastreo o plataformas de comunicación encriptadas, pero no todos tienen la capacidad económica o el conocimiento para hacer esta transición.

Además, en muchos países en desarrollo, el acceso a la tecnología ya está limitado, y con ello, las opciones para proteger la privacidad. En estos lugares, la infraestructura tecnológica a menudo no está diseñada para proteger los derechos de los usuarios, y la vigilancia gubernamental o corporativa es más común, exacerbando la brecha de privacidad.

Privacidad y vigilancia estatal

Otro aspecto que complica el debate es la creciente vigilancia por parte de los gobiernos. En nombre de la seguridad nacional y el combate al terrorismo, muchos estados han implementado programas de vigilancia masiva que, aunque diseñados para proteger a los ciudadanos, también los exponen a intrusiones en su vida privada. La vigilancia estatal a menudo se justifica por la necesidad de proteger a la sociedad, pero puede volverse un instrumento de control cuando se utiliza de manera abusiva.

La cuestión aquí es que la capacidad de resistir a la vigilancia estatal también está determinada por los recursos. Aquellos que pueden permitirse el uso de tecnologías que dificultan el seguimiento, como el cifrado de extremo a extremo o redes descentralizadas, pueden mantener un mayor nivel de privacidad que aquellos que dependen de los servicios proporcionados por gobiernos o corporaciones que cooperan con los programas de vigilancia.

¿Derecho o privilegio?

En teoría, la privacidad es y debe ser un derecho humano inalienable. Sin embargo, en la práctica, existen barreras significativas que impiden que todos disfruten de este derecho en igualdad de condiciones. El acceso a herramientas y recursos que protegen la privacidad está desigualmente distribuido, lo que convierte a la privacidad en un privilegio para quienes tienen los medios para protegerla.

Este hecho plantea un desafío crítico para las sociedades modernas: si la privacidad es realmente un derecho, entonces los gobiernos, las empresas y los actores de la sociedad civil deben trabajar juntos para garantizar que todos tengan acceso a las herramientas y el conocimiento necesario para proteger sus datos personales. Esto incluye no solo marcos legales fuertes, sino también educación y recursos accesibles que permitan a las personas tomar el control de su privacidad digital.

En última instancia, la privacidad no debería ser un privilegio, sino un derecho al que todos tengan acceso, independientemente de su situación económica, geográfica o tecnológica. Solo entonces podremos garantizar que la privacidad siga siendo un pilar fundamental de nuestras libertades individuales en el mundo digital.

Francisco Javier García Lorente
Project Manager

Las dos caras de una misma moneda: incidentes y avances en seguridad digital

Cibercrónica por Leire Cubo Arce

Recientemente, el mundo ha sido testigo de varios incidentes cibernéticos significativos que han puesto de relieve la fragilidad de las infraestructuras digitales y la necesidad de medidas de seguridad robustas. Estos eventos abarcan desde ataques a empresas reconocidas hasta avances importantes en la ciberseguridad.

Uno de los incidentes más destacados fue el ciberataque a **MoneyGram**, que tuvo lugar a finales de septiembre. Esta brecha de seguridad comprometió información sensible de los clientes, incluyendo nombres, números de Seguro Social y detalles de cuentas bancarias. La compañía tomó la decisión de desactivar sistemas para contener la brecha, lo que resultó en interrupciones del servicio que se extendieron hasta una semana.

También a finales de septiembre, varios puntos de acceso Wi-Fi en estaciones de tren del Reino Unido fueron objeto de un ataque DDoS que desvió a los usuarios a contenido inapropiado, subrayando las vulnerabilidades en la infraestructura pública.

Uno de los incidentes más importantes de octubre fue el ataque al proveedor de agua más grande de Estados Unidos, **American Water**, que sufrió una interrupción de servicios, aunque se ha confirmado que el suministro de agua no se vio comprometido. A pesar de ello, aún se investigan posibles fugas de datos y se desconocen detalles sobre el tipo de ataque que causó el incidente. Este ataque se suma a una tendencia preocupante de amenazas dirigidas a infraestructuras críticas.

Medios de comunicación estatales rusos enfrentaron ataques cibernéticos significativos que interrumpieron sus operaciones, lo que puso en evidencia las vulnerabilidades dentro de la infraestructura de los medios controlados por el estado. Por otro lado, en Francia, un operador hospitalario en Nantes sufrió un ciberataque que causó interrupciones operativas. Hasta el momento, no se han aclarado detalles sobre posibles filtraciones de datos.

Otro ataque notable fue el dirigido a **Casio**, el famoso fabricante japonés de electrónica. Un ataque de *ransomware* impactó sus operaciones en Tokio, aunque no se dieron a conocer detalles específicos sobre posibles violaciones de datos.

En la India, un ataque de *malware* afectó a los sistemas gubernamentales en Uttarakhand, lo que generó preocupaciones sobre las medidas de ciberseguridad en las instituciones estatales.

Adicionalmente, importantes puertos en Bélgica enfrentaron interrupciones debido a un ataque DDoS, poniendo de manifiesto la vulnerabilidad de la infraestructura crítica ante los cibercriminales.

En un contexto más amplio, **T-Mobile** llegó a un acuerdo con la FCC para pagar $15.75 millones en respuesta a varias brechas de seguridad que expusieron datos de millones de clientes, comprometiéndose a invertir en la mejora de sus sistemas de ciberseguridad.

Kaspersky se vio envuelta en controversia por reemplazar automáticamente su software antivirus con UltraAV, provocando preocupación entre los usuarios, aunque esto formaba parte de un esfuerzo para proteger a los usuarios de Windows tras su salida del mercado.

En otro ámbito, **Cryptex**, un intercambio de criptomonedas fue sancionado por procesar fondos de actividades cibernéticas criminales, lo que subraya el enfoque creciente de los reguladores en la ciberseguridad.

Por otro lado, está la reciente detención de cuatro personas con vínculos al grupo de *ransomware* **LockBit**, poniendo de relieve la cooperación internacional en la lucha contra el cibercrimen, lo que podría ser un paso significativo hacia la desarticulación de estas organizaciones maliciosas.

Los recientes avances en herramientas de diseño 3D, como las presentadas por **Meta**, destacan la creciente necesidad de abordar los desafíos de ciberseguridad que acompañan a estas innovaciones. Con la democratización de plataformas que facilitan la creación de contenido digital, se incrementa el riesgo de ciberataques que pueden manipular modelos o introducir malware en los entornos virtuales.

A medida que los ataques se vuelven más sofisticados, es crucial que las organizaciones fortalezcan sus medidas de seguridad y mantengan una vigilancia constante ante posibles brechas. La inversión en tecnología de ciberseguridad y la educación continua son pasos esenciales para proteger tanto a las empresas como a sus usuarios.

A pesar de estos incidentes, no todo son malas noticias en el ámbito de la ciberseguridad. En octubre de 2024, varias empresas anunciaron importantes avances tecnológicos. **CrowdStrike** lanzó Charlotte AI, un asistente impulsado por IA que promete mejorar la productividad de los analistas de seguridad al automatizar la detección y respuesta a amenazas.

Por su parte, **Fortinet** presentó FortiAI, una herramienta diseñada para acelerar el análisis de incidentes, facilitando a las organizaciones interpretar eventos de seguridad y generar información útil de manera más eficiente.

Además, **Palo Alto Networks** continúa innovando con su plataforma Cortex XSIAM, que utiliza tecnologías avanzadas de IA para crear una experiencia de operaciones de seguridad totalmente autónoma, mejorando la detección y remediación de amenazas complejas.

SentinelOne también se unió a la vanguardia de la ciberseguridad con su plataforma Singularity Unity, que mejora la capacidad de caza de amenazas, permitiendo que los equipos de seguridad manejen volúmenes mayores de ataques con mayor precisión.

Estos avances en IA, cifrado y autenticación destacan el esfuerzo constante por fortalecer las defensas digitales ante el panorama de amenazas cada vez más sofisticadas. La ciberseguridad no es solo una preocupación para el sector tecnológico, sino que impacta a todas las industrias y servicios.

Leire Cubo Arce
Cybersecurity Consultant

Privacidad por diseño y ciberseguridad

Artículo por Fernando del Valle Rodríguez

En la era de la digitalización, la privacidad no puede considerarse un elemento separado de la ciberseguridad. Los usuarios confían cada vez más en servicios digitales para gestionar sus datos personales, mientras que las amenazas cibernéticas continúan evolucionando con el objetivo de explotar esta información. Por ello, integrar la privacidad desde el diseño de cualquier proyecto de ciberseguridad es esencial no solo para proteger a los usuarios, sino también para cumplir con regulaciones cada vez más estrictas.

Diferencias e interdependencia

Aunque la privacidad y la ciberseguridad están estrechamente relacionadas, es fundamental entender que no son lo mismo. La ciberseguridad se enfoca en proteger sistemas, redes y datos contra ciberataques o daños accidentales, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. Por otro lado, la privacidad se centra en la correcta gestión y protección de los datos personales, asegurando que se manejen de acuerdo con los derechos de los individuos.

Sin embargo, ambas disciplinas son interdependientes. Una deficiente protección de la privacidad puede derivar en brechas de seguridad, y viceversa. Por ejemplo, un ciberataque a una base de datos que contiene información personal no encriptada podría exponer datos sensibles que luego se utilizan para fraude o comercialización en mercados ilegales. Del mismo modo, una mala gestión de la privacidad puede facilitar ataques como el phishing. Por tanto, es crucial diseñar medidas de ciberseguridad que también protejan la privacidad.

El concepto de "Privacidad por Diseño“

El enfoque de Privacidad por Diseño (*Privacy by Design*) implica integrar medidas de protección de datos desde el inicio del desarrollo de un sistema o proyecto, incluidos los de ciberseguridad. Este enfoque proactivo busca que la privacidad no sea un complemento añadido al final, sino una parte integral del ciclo de vida del proyecto, desde su concepción hasta su implementación.

Además de facilitar el cumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD), Privacidad por Diseño previene riesgos innecesarios. No hacerlo desde el principio puede generar retrasos, cambios costosos y sanciones debido a la falta de cumplimiento, así como pérdida de confianza del cliente y daños reputacionales. Por lo tanto, el diseño proactivo en la protección de datos no solo es una cuestión de cumplimiento legal, sino también una estrategia clave para el éxito a largo plazo.

Beneficios de integrar la privacidad en proyectos de ciberseguridad

Incorporar la privacidad en los proyectos de ciberseguridad genera importantes beneficios:

- **Cumplimiento normativo**: Las regulaciones sobre protección de datos, como el Reglamento General de protección de Datos (RGPD) o la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), obligan a las organizaciones a proteger adecuadamente los datos personales. La integración de la privacidad desde el inicio facilita el cumplimiento no solo de estas normativas, sino también de otras como NIS2, DORA, ENS o estándares internacionales como ISO 27001 e ISO 29100.

- **Reducción de riesgos**: Las violaciones de privacidad no solo conllevan pérdidas económicas, sino que también dañan gravemente la reputación de las empresas, lo que puede ser difícil de reparar. Al integrar la privacidad desde el principio, se minimizan tanto los riesgos técnicos como los legales.

- **Confianza del cliente**: Los usuarios son cada vez más conscientes del valor de su información personal y prefieren servicios que prioricen la protección de su privacidad. Las empresas que lo hagan generarán mayor confianza en sus clientes, lo que a su vez puede traducirse en una ventaja competitiva clave.

Estrategias para incorporar la privacidad en proyectos de ciberseguridad

Para asegurar una correcta implementación de la privacidad en proyectos de ciberseguridad, es necesario adoptar las siguientes prácticas:

- **Análisis de necesidades del cliente y del proyecto**: El primer paso es analizar las necesidades del proyecto respecto a la privacidad. Si no se manejan datos personales, puede que no sea necesario implementar medidas específicas, pero si se gestionan, la privacidad debe ser prioritaria desde el comienzo.

- **Análisis de riesgos y evaluación de impacto**: Determinar los riesgos potenciales para la privacidad en las fases iniciales permite establecer medidas correctivas a tiempo, minimizando los riesgos y asegurando que el tratamiento de los datos se realice de forma segura.

- **Minimización de datos**: Recoger solo los datos estrictamente necesarios y establecer límites claros sobre su retención es fundamental para reducir riesgos de seguridad y garantizar el cumplimiento de las normativas.

- **Incorporación de derechos de protección de datos de los usuarios**: Incluir medidas que garanticen los derechos de los usuarios, como el acceso, rectificación y eliminación de sus datos, evita modificaciones costosas y asegura el cumplimiento normativo.

La clave de estas estrategias es el trabajo conjunto entre las áreas de ciberseguridad y privacidad, garantizando una comunicación fluida y un enfoque integral para la protección de los datos.

Desafíos al integrar la privacidad en ciberseguridad

A pesar de los beneficios, integrar la privacidad en proyectos de ciberseguridad presenta ciertos desafíos:

- **Costos iniciales**: Implementar medidas avanzadas de privacidad desde las primeras fases puede aumentar los costos en términos de tiempo, recursos y tecnología. Sin embargo, estos costos son menores comparados con los gastos derivados de sanciones o modificaciones forzadas en fases avanzadas del proyecto.
- **Complejidad técnica**: Algunas medidas, como la anonimización o el cifrado fuerte, pueden ser difíciles de implementar en sistemas complejos, especialmente en infraestructuras heredadas. Sin embargo, estas medidas son cruciales para prevenir filtraciones que conlleven daños financieros y reputacionales.
- **Falta de capacitación**: Muchos equipos de ciberseguridad no tienen la formación adecuada en protección de datos personales. Incluir expertos en privacidad, como el departamento de Legal & Compliance, es esencial para garantizar que las normativas y mejores prácticas se integren adecuadamente.

Tendencias futuras: automatización y nuevas normativas

El futuro de la privacidad y la ciberseguridad pasa por la automatización. Herramientas basadas en inteligencia artificial permitirán detectar y mitigar amenazas a la privacidad de forma más proactiva y eficiente. Además, normativas como el Reglamento de Inteligencia Artificial exigirán a las organizaciones adaptarse con rapidez, especialmente en su interconexión con las leyes y normas de protección de los datos personales.

La integración de la privacidad en los proyectos de ciberseguridad es hoy más que una buena práctica, es una necesidad. Adoptar el enfoque de Privacidad por Diseño garantiza la protección tanto de la seguridad como de la privacidad de los datos, facilitando el cumplimiento normativo y ganando la confianza de los clientes.

Las empresas que prioricen la protección de datos estarán mejor preparadas para enfrentar los retos de esta era digital.

Fernando del Valle Rodríguez
Cybersecurity Consultant

El auge de las plataformas *low-code/no-code* y los retos de seguridad: una nueva era de desarrollo

Tendencias por Damián Pardiñas Rodríguez

En los últimos años, las plataformas *Low-Code/No-Code* (LCNC) han revolucionado la manera en que las empresas desarrollan aplicaciones. Herramientas como Retool, Power Platform de Microsoft, y otras similares permiten a personas con poca o ninguna experiencia en programación crear aplicaciones funcionales de manera rápida y eficiente.

Este enfoque ha democratizado el desarrollo, facilitando la creación de soluciones tecnológicas dentro de las organizaciones y acelerando la innovación. Sin embargo, a pesar de sus múltiples beneficios, las plataformas LCNC presentan desafíos significativos en términos de seguridad, un aspecto crucial que no puede pasarse por alto.

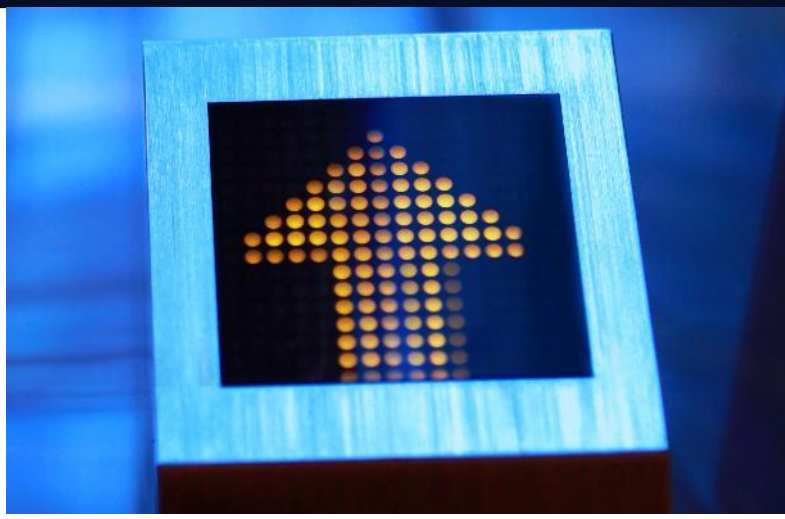
Un auge impulsado por la necesidad de agilidad

La creciente demanda de aplicaciones personalizadas en sectores como el comercio, la educación y la salud ha impulsado la adopción masiva de plataformas LCNC. Estas herramientas ofrecen a las organizaciones la posibilidad de responder rápidamente a las necesidades del mercado, sin depender exclusivamente de equipos de desarrollo especializados. Un buen ejemplo es **Retool**, una plataforma de desarrollo *low-code* que permite a las empresas crear interfaces internas con facilidad, aprovechando datos y sistemas existentes. De manera similar, **Microsoft Power Platform** ofrece a las organizaciones la capacidad de crear aplicaciones, automatizar flujos de trabajo y analizar datos con una mínima intervención de desarrolladores tradicionales.

El atractivo principal de las plataformas LCNC radica en su simplicidad y capacidad para reducir el "*time to market*". Sin embargo, esta simplicidad también trae consigo nuevos riesgos de seguridad. Aunque las plataformas facilitan el desarrollo, gran parte de la seguridad del código no recae en los desarrolladores de las aplicaciones, sino en las plataformas mismas, lo que plantea una serie de desafíos importantes.

El impacto de la seguridad en las plataformas LCNC: OWASP y el *Top Ten*

La rápida adopción de las plataformas LCNC ha llamado la atención de la **Open Web Application Security Project** (**OWASP**), una organización reconocida por su trabajo en la identificación de vulnerabilidades de seguridad en aplicaciones.



OWASP recientemente lanzó un ***Top Ten*** dedicado específicamente a los riesgos de seguridad de plataformas *low-code/no-code*, destacando los principales desafíos a los que se enfrentan las organizaciones que dependen de estas tecnologías.

Las tres principales vulnerabilidades de este listado son:

1. **Suplantación de cuentas (*Account Impersonation*)**: La facilidad para delegar privilegios dentro de las plataformas LCNC a menudo genera escenarios donde las credenciales y permisos no son gestionados de manera adecuada, permitiendo a los atacantes suplantar identidades y acceder a recursos críticos.
2. **Mal uso de la autorización (*Authorisation Misuse*)**: La incorrecta configuración de permisos y roles dentro de las aplicaciones LCNC es uno de los riesgos más comunes, permitiendo que usuarios no autorizados accedan a datos o funciones que deberían estar restringidas.
3. **Filtración de datos y consecuencias inesperadas (*Data Leakage and Unexpected Consequences*)**: En muchas ocasiones, las plataformas LCNC permiten la manipulación de datos sin un control adecuado de la seguridad, lo que puede derivar en la exposición involuntaria de información sensible o la creación de situaciones imprevistas que comprometan la integridad del sistema.

Este nuevo listado de OWASP refleja cómo los riesgos tradicionales de seguridad han evolucionado en el contexto de las plataformas LCNC, donde los problemas de autenticación y autorización, comúnmente gestionados por desarrolladores experimentados, ahora deben ser controlados por la plataforma misma.

Herramientas de análisis para LCNC: un nuevo aliado

Ante estos riesgos, están emergiendo nuevas herramientas que permiten a las empresas monitorizar y analizar las aplicaciones creadas en plataformas LCNC. Estas herramientas están diseñadas específicamente para detectar vulnerabilidades, analizar configuraciones y validar que las aplicaciones cumplan con los estándares de seguridad de la organización. Un ejemplo de este tipo de soluciones son los servicios de monitorización de seguridad LCNC que auditan las aplicaciones en tiempo real, detectando problemas antes de que puedan ser explotados por actores malintencionados.

Ejemplos de estas soluciones incluyen **Zenity** y **Valence Security**, que ayudan a auditar y gestionar la seguridad de las aplicaciones desarrolladas en plataformas LCNC.

Estas herramientas resultan críticas en un entorno donde la seguridad del código recae, en gran medida, en la propia plataforma y no tanto en los desarrolladores. Esto representa una diferencia fundamental con respecto a los desarrollos tradicionales, donde los desarrolladores tenían el control directo sobre cada línea de código y podían implementar directamente prácticas de seguridad robustas.

En el caso de las plataformas LCNC, la mayoría de las organizaciones dependen casi por completo de los mecanismos de seguridad incorporados en la plataforma, lo que aumenta la necesidad de confiar en proveedores que tengan un historial sólido en seguridad.

Nuevos horizontes y ciber-responsabilidad

Las plataformas *low-code/no-code* han abierto nuevas oportunidades para acelerar la innovación y mejorar la eficiencia en el desarrollo de aplicaciones. Sin embargo, este enfoque tiene implicaciones importantes para la seguridad. Los riesgos identificados por OWASP destacan que, aunque las plataformas LCNC son poderosas, también pueden ser vulnerables si no se gestionan adecuadamente.

La responsabilidad de la seguridad, que tradicionalmente recaía en los desarrolladores, ahora se transfiere en gran medida a la plataforma, lo que subraya la importancia de seleccionar herramientas seguras y de monitorizar continuamente las aplicaciones para mitigar posibles riesgos.

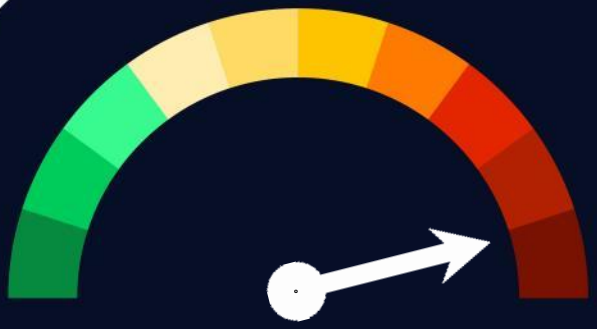
Las organizaciones deben ser conscientes de estos desafíos y adoptar un enfoque proactivo en la protección de sus aplicaciones, integrando herramientas especializadas y asegurándose de que las plataformas LCNC utilizadas cumplan con los más altos estándares de seguridad.

Damián Pardiñas Rodríguez
Cybersecurity Expert Analyst

Vulnerabilidades

Vulnerabilidad crítica en Cisco Small Business

Fecha: 2 de octubre de 2024
CVE: CVE-2024-20518



CVSS: 9.1

CRÍTICA

Descripción

La vulnerabilidad crítica CVE-2024-20518, que afecta a varios modelos de Cisco Small Business, permitirían a un atacante ejecutar código arbitrario e incluso causar un ataque DoS.

Estas vulnerabilidades están basadas en la interfaz de administración de los *routers* Cisco Small Business y con ellas, el atacante incluso podría ejecutar este código de manera remota.

Cisco ha manifestado que no tendrán actualizaciones para estos modelos debido a que están fuera de fecha de mantenimiento y soporte.

Solución

Aunque el fabricante no publicará ningún parche de seguridad para corregir estas vulnerabilidades, este facilitó los siguientes consejos para evitar esta explotación.

- Desactivar la gestión remota del dispositivo, esto permitiría que solo se pueda acceder a estos dispositivos vía red LAN y no externamente.
- Bloquear el acceso a los puertos 443 y 60443, esto implicaría la creación de reglas de tráfico de red para estos bloqueos.

En el apartado “Referencias” se encuentra más información al respecto para estas mitigaciones.

Productos afectados

La vulnerabilidad afecta a las siguientes versiones:

- RV042 Routers VPN WAN duales
- RV042G Routers VPN WAN Gigabit Duales
- RV320 Dual Gigabit WAN VPN Routers
- RV325 Routers VPN WAN Gigabit duales

Referencias

- incibe.com
- sec.cloudapps.cisco.com
- cvedetails.com

Vulnerabilidades

Vulnerabilidad en Siemens SINEC Security Monitor

Fecha: 8 de octubre de 2024
CVE: CVE-2024-47553 y 1 más

CVSS: 9.9

CRÍTICA

Descripción

El fabricante Siemens ha revelado varias vulnerabilidades que afectan a su producto, SINEC Security Monitor, siendo dos de ellas de severidad crítica:

- CVE-2024-47553: gracias a un fallo en la entrada del comando "ssmtl-client", un atacante remoto autenticado con privilegios limitados podría lanzar código arbitrario con permisos de *root*.
- CVE-2024-47562: durante la ejecución del comando "sstml-client" existen errores de gestión en elementos especiales, lo que provocaría que puedan lanzarse comandos con usuarios privilegiados en el SO subyacente.

Solución

Con el fin de corregir estas vulnerabilidades, Siemens recomienda a los usuarios afectados que actualicen a la versión 4.9.0 o a otra posterior.

Además, como medida extra de seguridad, Siemens sugiere que los usuarios cuenten con una buena protección en el acceso a la red y recomiendan que se basen en sus propias directivas para configurar sus entornos.

Productos afectados

Las 2 vulnerabilidades anteriores afectan al producto SINEC Security Monitor, concretamente en todas las versiones anteriores a 4.9.0.

Referencias

- tenable.com
- siemens.com
- incibe.es

Parches de seguridad de octubre de Microsoft

Fecha: 8 de octubre de 2024
CVE: CVE-2024-43468 y 116 más

Crítica

Descripción

Microsoft ha publicado su actualización mensual de seguridad donde recoge 117 vulnerabilidades; 3 de ellas críticas, 110 importantes, 3 moderadas y 1 baja. Las vulnerabilidades con mayor criticidad son:

- CVE-2024-43468: es la vulnerabilidad más crítica. Se ha detectado en Microsoft Configuration Manager. Permitiría a un atacante sin autenticar ejecutar comandos de forma remota en el servidor.
- CVE-2024-38124: vulnerabilidad de elevación de privilegios en Netlogon de Windows que podría permitir a un atacante obtener acceso no autorizado a los recursos del sistema.

Productos afectados

La actualización de seguridad de octubre incluye parches para los siguientes recursos, entre otros:

- Windows 10 Versiones 21H2, 22H2
- Windows Server 2022
- Windows 11 Versión 24H2
- Windows Server 2008
- Windows Server 2008

La lista completa de productos afectados puede consultarse en el siguiente enlace: microsoft.com

Solución

Se recomienda aplicar los parches de seguridad de octubre de 2024 de Microsoft lo antes posible.

Referencias

- microsoft.com
- news.sophos.com

Actualizaciones de seguridad para vulnerabilidades en GitLab

Fecha: 9 de octubre de 2024
CVE: CVE-2024-9164 y 7 más

Crítica

Descripción

Veeam ha lanzado un nuevo boletín con actualizaciones de seguridad que abordan 8 vulnerabilidades, entre ellas críticas y altas, de sus productos GitLab Community Edition (CE) y Enterprise Edition (EE).

Entre las vulnerabilidades corregidas se encuentra la vulnerabilidad crítica CVE-2024-9164 (con un score de 9.6) Esta vulnerabilidad afecta a Gitlab EE y permitiría a un atacante ejecutar pipelines y hacerse pasar por un usuario legítimo para modificar cualquier rama del repositorio.

Estos pipelines afectados son procesos automatizados que realizan tareas como compilar, probar e implementar código, normalmente solo para usuarios con permisos adecuados.

Productos afectados

Las vulnerabilidades publicadas en el boletín afectan a los siguientes productos (con sus versiones correspondientes):

- GitLab Community Edition (CE):
  - Versiones anteriores a la 17.4.2.
  - Versiones anteriores a la 17.3.5.
  - Versiones anteriores a la 17.2.9.
- Enterprise Edition (EE):
  - Versiones anteriores a la 17.4.2.
  - Versiones anteriores a la 17.3.5.
  - Versiones anteriores a la 17.2.9.

Solución

Se recomienda encarecidamente que todas las instalaciones que se ejecuten en una versión afectada se actualicen lo antes posible según el boletín de seguridad ed GitLab.

Referencias

- about.gitlab.com
- bleepingcomputer.com
- incibe.es

Eventos

Benelux Cyber Summit
5 de noviembre

El Benelux Cyber Summit es un evento anual que reúne a líderes de TI y ciberseguridad de Europa para debatir sobre las últimas tendencias y tecnologías en ciberseguridad. El evento incluye estudios de caso, paneles de discusión y sesiones de *networking*, con un enfoque en temas como la protección de infraestructuras críticas, la automatización de la seguridad y el uso de inteligencia artificial para detectar amenazas. También aborda normativas regionales como el RGPD y la Directiva NIS2, destacando la importancia de la colaboración entre el sector público y privado para combatir el cibercrimen.

Enlace

XXVI Jornada Internacional de Seguridad de la Información
14 de noviembre

ISMS Forum Spain organiza las Jornadas Internacionales de Seguridad de la Información al año, que son un punto de encuentro de discusión y debate entre representantes de todos los actores implicados en el sector. Las Jornadas Internacionales congregan a ponentes nacionales e internacionales de primer nivel para abordar los temas de mayor actualidad y especial relevancia de la Seguridad de la Información. Todo ello, en un entorno que facilita las relaciones profesionales y el intercambio de conocimientos.

Enlace

Cybersecurity & Identification 2024 (CISO CTO WORLD)
21 de noviembre

El evento Cybersecurity & Identification, que se llevará a cabo el 21 de noviembre de 2024 en el Hotel Ilunion Atrium de Madrid, se centra en la integración de la ciberseguridad y la gestión de identidades. La jornada abordará temas como el impacto de la inteligencia artificial en la ciberseguridad, los desafíos en la gestión de identidades y la protección de datos personales. También se discutirán regulaciones globales y locales y cómo las nuevas soluciones de seguridad pueden ser implementadas en sistemas en la nube.

Enlace

XVII Jornadas STIC CCN-CERT
26-28 de noviembre

Madrid será sede de las XVIII Jornadas STIC CCN-CERT y las VI Jornadas de Ciberdefensa ESPDEF-CERT, organizadas por el Centro Criptológico Nacional (CNI) y el Mando Conjunto del Ciberespacio (MCCE). Este evento, en colaboración con RootedCON, reunirá a expertos de la ciberseguridad para debatir sobre amenazas, nuevas tecnologías y ciberdefensa activa. Se impartirán talleres prácticos y conferencias en seis salas temáticas, cubriendo desde análisis forense hasta *blockchain*, contando con la participación de las principales empresas tecnológicas y organismos internacionales.

Enlace

Recursos

➢ CylancePROTECT: Inteligencia Artificial y Aprendizaje Automático

CylancePROTECT es una herramienta que busca aprovechar la técnica de aprendizaje automático para la detección y prevención de malware en tiempo real. A diferencia de los antivirus tradicionales u otras aplicaciones antivirus conocidas que se basan en firmas, CylancePROTECT trabaja para identificar ataques basándose en el comportamiento exhibido por ataques desconocidos.

Enlace

➢ Seguridad Zero Trust

El enfoque de Seguridad Zero Trust postula que ninguna solicitud de acceso es confiable por defecto, lo que se traduce en verificar cada intento de acceso en la red. Este concepto se está convirtiendo rápidamente en la estrategia de defensa de red empresarial más buscada, ya que reduce cualquier riesgo de brechas de seguridad al asegurar que solo usuarios y dispositivos autorizados puedan acceder a recursos críticos.

Enlace

➢ Apolo

Apolo es una herramienta SaaS que se concentra en automatizar la ciberseguridad diaria y el cumplimiento regulatorio. Promete identificar vulnerabilidades e incluso tiene la capacidad de capacitar a los empleados que son nuevos en ciberseguridad. La amplia perspectiva de la solución permite que la seguridad de las organizaciones y sus partes interesadas esté a un alto nivel y cumpla con las regulaciones de una manera rentable.

Enlace

➢ Proofpoint

El sistema ha mejorado recientemente las capacidades de detección y bloqueo de phishing utilizando tecnologías de vanguardia, lo que permite una respuesta más rápida a las amenazas. La plataforma todo en uno previene que estas organizaciones sufran numerosos ataques dirigidos, asegurando una comunicación segura y confiable dentro del ámbito de la empresa.

Enlace

➢ Directiva NIS2

La Directiva NIS2 es una normativa europea que establece requisitos más estrictos para la ciberseguridad en las organizaciones. Esto implica que muchas empresas están implementando nuevas herramientas y medidas para cumplir con las regulaciones, fortaleciendo así su postura de seguridad y reduciendo el riesgo de incidentes cibernéticos.

Enlace

➢ Legislación de Resiliencia Cibernética

La propuesta de la Ley de Resiliencia Cibernética refuerza los requisitos de ciberseguridad para los productos digitales, lo que ha incrementado el desarrollo de herramientas que cumplen con las leyes mencionadas. Esta legislación tiene como objetivo mejorar la capacidad de las organizaciones para resistir y recuperarse de ciberataques, con el fin de promover un entorno digital seguro y confiable.

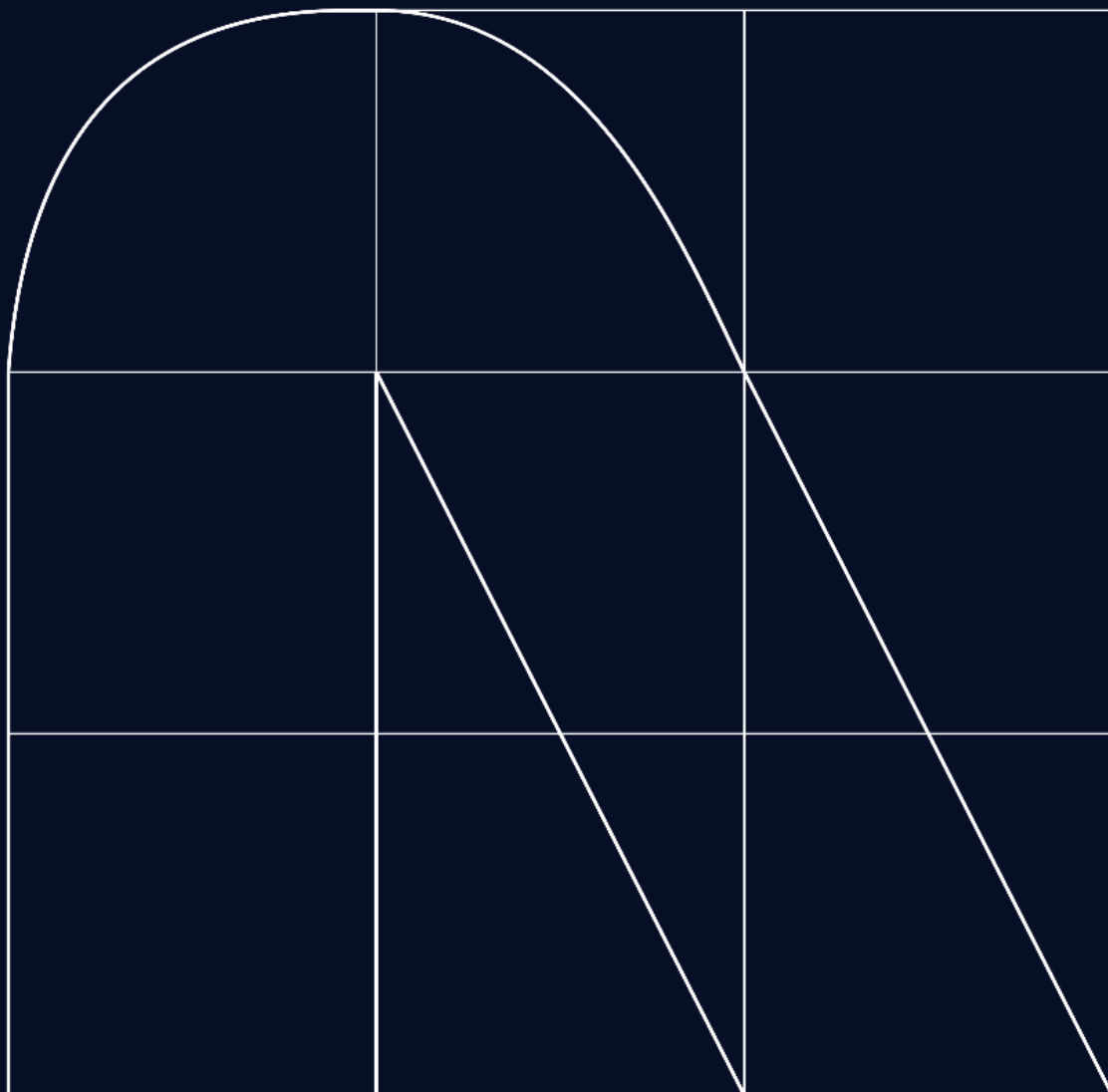
Enlace

➢ OSSEC

OSSEC se centra en el Sistema de Detección de Intrusiones en Hosts (HIDS) que realiza la detección de intrusiones a nivel de host, análisis de logs, verificación de integridad y detección de rootkits. Es una aplicación de código abierto y ofrece una protección suficiente de software más todas las vulnerabilidades de código abierto cuando se configura adecuadamente. Precisamente, denunciaron la API de monitoreo de logs y detectaron que no hacía falta incluir la API Offense, por lo que deshabilitaron la funcionalidad de edición para ambas APIs.

Enlace

Suscríbete a RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com