UNIDAD DE CIBERDEFENSA NAVAL

BOLETÍN SEMANAL DE CIBERSEGURIDAD

DEL 30 DICIEMBRE AL 19 DE ENERO

Las consecuencias de una brecha de seguridad en la actualidad son cada vez más severas, poniendo en riesgo no solo la confidencialidad de la información sino también la reputación y la continuidad operativa de las organizaciones. El cibercrimen ha evolucionado hasta convertirse en una amenaza global que exige una respuesta proactiva. Por ello, la Unidad de Ciberdefensa Naval emite el boletín semanal de ciberseguridad, dentro del mismo se erigen como herramientas indispensables para mantenerse al día sobre las últimas vulnerabilidades y adoptar medidas preventivas oportunas. Al comprender las amenazas emergentes y aplicar las recomendaciones de los expertos, las organizaciones pueden mitigar significativamente los riesgos cibernéticos y proteger sus activos más valiosos.

03 DE ENERO DE2025

VULNERABILIDAD CVE-2024-9140

Es una vulnerabilidad crítica que afecta a dispositivos de red de Moxa, incluidos routers celulares, routers seguros y dispositivos de seguridad. Esta vulnerabilidad permite la inyección de comandos del sistema operativo (CWE-78) debido a la falta de restricción y neutralización adecuada de elementos especiales utilizados en comandos del sistema. Un atacante remoto no autenticado podría explotar esta vulnerabilidad para ejecutar código arbitrario en los dispositivos afectados, comprometiendo su seguridad y funcionalidad.

.07 DE ENERO DE 2025

VULNERABILIDAD CVE-2025-22133

vulnerabilidad crítica en WeGIA, un gestor web para instituciones benéficas, que afecta versiones anteriores a la 3.2.8. Se recomienda actualizar a la última versión para mitigar los riesgos asociados a esta vulnerabilidad.

09 DE ENERO DE 2025

VULNERABILIDAD CVE-2025-54887

Es una vulnerabilidad crítica que afecta a los routers TP-Link TL-WR940N V3 y V4 con firmware versión 3.16.9 y anteriores. La vulnerabilidad consiste en un desbordamiento de búfer a través de los parámetros dnsserver1 y dnsserver2 en el archivo /userRpm/Wan6to4TunnelCfgRpm.htm.

Un atacante autenticado puede explotar esta vulnerabilidad para ejecutar código arbitrario en el dispositivo, obteniendo privilegios de usuario raíz en el sistema. Este fallo representa un alto riesgo de compromiso total del dispositivo.

15 DE ENERO DE 2025

VULNERABILIDAD CVE-2025-54887

Se ha identificado una vulnerabilidad en GitHub Desktop (todas las versiones anteriores a la 3.4.12) que podría permitir a un atacante exfiltrar credenciales sensibles. Esto ocurre cuando un usuario clona un repositorio utilizando una URL remota maliciosamente diseñada, lo que resulta en la transmisión inadvertida de credenciales del usuario hacia un host controlado por el atacante.

Contacto para reportes:

Ante un incidente de seguridad informática se deberá reportar al correo csirt@armada.mil.ec, o mediante la página csirt.armada.mil.ec seleccionando en la opción del menú “Reportar Incidente”.

¡Reporta Aquí!