Del 1 al 14 de septiembre

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

GRUPO spri TALDEA

Basque CyberSecurity Centre

Múltiples vulnerabilidades en HPE SANnav Management Software

HPE ha notificado 48 vulnerabilidades en su producto SANnav Management Software, 7 de ellas críticas y el resto repartidas entre altas, medias y críticas.

Avisos técnicos - Del 1 al 14 de septiembre

Múltiples vulnerabilidades en ARCONTE Áurea de Fujitsu

INCIBE ha coordinado la publicación de 5 vulnerabilidades que afectan a Arconte Áurea, de Fujitsu, un software para la grabación de vistas judiciales, descubiertas por Pablo Arias Rodriguez y Jorge Alberto Palma Reyes del CSIRT-CV.

A estas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad.

Avisos técnicos - Del 1 al 14 de septiembre

Referencia directa insegura a objetos en ZEM800 de ZKTeco

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a ZEM800 de ZKTeco, un dispositivo de seguridad para el control de acceso y de fichaje, la cual ha sido descubierta por David Utón Amaya, del equipo de Telefónica Tech.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y tipo de vulnerabilidad CWE.

Boletín de seguridad de Android de septiembre de 2023

El boletín de Android, relativo a septiembre de 2023, soluciona múltiples vulnerabilidades de severidad crítica y alta que afectan a su sistema operativo, así como múltiples componentes, que podrían permitir a un atacante realizar una escalada de privilegios, divulgar información y provocar una denegación de servicio (DoS) o hacer una ejecución de código remota (RCE).

Avisos técnicos - Del 1 al 14 de septiembre

Múltiples vulnerabilidades en Secret Server de Delinea

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a Secret Server, de Delinea, un software de gestión de accesos privilegiados (PAM), descubiertas por Héctor de Armas Padrón (@3v4SI0N).

A estas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad.

Avisos técnicos - Del 1 al 14 de septiembre

Omisión de autenticación en Cisco BroadWorks y servicios Xtended

Cisco ha publicado una vulnerabilidad de severidad crítica que podría permitir que un atacante remoto, no autenticado, falsifique las credenciales necesarias para acceder a un sistema afectado.

Avisos técnicos - Del 1 al 14 de septiembre

Múltiples vulnerabilidades en controladores y puertas de enlace de HPE Aruba

HP ha publicado 3 vulnerabilidades de severidad alta que podrían permitir a un atacante obtener acceso y cambiar información confidencial subyacente en el controlador afectado, lo que comprometería completamente el sistema.

Avisos técnicos - Del 1 al 14 de septiembre

Múltiples vulnerabilidades en HPE OneView

Sina Kheirkhah (@SinSinology), de Summoning Team (@SummoningTeam), en colaboración con Trend Micro Zero Day Initiative, ha reportado una vulnerabilidad de severidad crítica. Además, HPE ha publicado 2 vulnerabilidades más, de severidad alta y media respectivamente.

Avisos técnicos - Del 1 al 14 de septiembre

Múltiples vulnerabilidades en Open5GS

INCIBE ha coordinado la publicación de 4 vulnerabilidades que afectan a Open5GS, una implementación de núcleo de red 5G y 4G, descubiertas por Pablo Valle Alvear, del equipo de Titanium Industrial Security.

A estas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad.

Avisos técnicos - Del 1 al 14 de septiembre

Oday de tipo ejecución de código arbitrario en ImageIO y Wallet de Apple

Un investigador, de la escuela Munk de la Universidad de Toronto, junto a Apple han informado de 2 vulnerabilidades, de tipo 0day, que podría permitir a un atacante ejecutar código arbitrario.

Avisos técnicos - Del 1 al 14 de septiembre

Actualizaciones de seguridad de Microsoft de septiembre de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 12 de septiembre, consta de 59 vulnerabilidades (con CVE asignado), calificadas 47 como importantes y 12 medias.

Avisos técnicos - Del 1 al 14 de septiembre

Actualización de seguridad de SAP de septiembre de 2023

SAP han publicado varias actualizaciones de seguridad en diferentes productos en su comunicado mensual.

Avisos técnicos - Del 1 al 14 de septiembre

Denegación de servicio en PAN-OS de Paloalto

Ben Cartwright-Cox ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante remoto causar una denegación de servicio (DoS) en los productos afectados.

Múltiples vulnerabilidades en QSige de IDM Sistemas

INCIBE ha coordinado la publicación de 7 vulnerabilidades que afectan a QSige de IDM Sistemas, un sistema inteligente de gestión de esperas, descubiertas por Pablo Arias Rodríguez, Jorge Alberto Palma Reyes y Rubén Barberá Pérez, investigadores del Red Team del CSIRT-CV. Mención especial a todo el equipo del CSIRT-CV.

A estas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad.

Avisos técnicos - Del 1 al 14 de septiembre

Cross-site Scripting en productos FortiOS y FortiProxy de Fortinet

William Costa, del equipo CSE de Fortinet, ha notificado una vulnerabilidad de severidad alta que podría permitir que un atacante autenticado desencadene la ejecución de código JavaScript malicioso en una página de gestión de invitados.

Avisos técnicos - Del 1 al 14 de septiembre