Febrero 2022

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

Vulnerabilidad en IBM Security Verify Access

IBM ha detectado una vulnerabilidad crítica en su producto Security Verify Access.

Avisos técnicos - Febrero 2022

Múltiples vulnerabilidades en Samba

Varios investigadores han reportado 3 vulnerabilidades en Samba: 1 de severidad crítica, 1 alta y 1 media. Un atacante podría filtrar información, ejecutar código y suplantar servicios arbitrarios, en caso de explotarlas.

Vulnerabilidad de ataques basados en XXE en productos HP

HP ha publicado una vulnerabilidad de severidad crítica, por la que un atacante podría realizar ataques basados en XXE (XML External Entity).

Avisos técnicos - Febrero 2022

Múltiples vulnerabilidades en InsydeH2O UEFI de Insyde

El equipo efiXplorer de Binarly investigó y reportó 23 vulnerabilidades de gestión de memoria en System Management Mode (SMM) a Insyde Software. Un atacante local (en algunos casos un atacante remoto) con privilegios administrativos podría utilizar malware para invalidar características de seguridad hardware, instalar software persistente y crear backdoors para filtrar información sensible.

Avisos técnicos - Febrero 2022

Múltiples vulnerabilidades en productos Cisco

Se han publicado múltiples vulnerabilidades en productos de Cisco que podrían permitir a un atacante ejecutar código arbitrario, escalar privilegios, ejecutar comandos arbitrarios, omisión de autenticación, ejecutar software no firmado o denegar el servicio.

Avisos técnicos - Febrero 2022

Múltiples vulnerabilidades en IBM Planning Analytics

IBM ha reportado 11 vulnerabilidades: 2 críticas, 2 altas, 3 medias y 4 bajas, por las que un atacante podría causar un impacto en la confidencialidad, en la integridad y en la disponibilidad, una denegación de servicio, obtener información sensible, desbordar un búfer, ejecutar código arbitrario, acceder a directorios restringidos, realizar una ejecución remota de código o tomar el control del sistema.

Avisos técnicos - Febrero 2022

Wocu Monitoring es vulnerable a Cross-Site Scripting (XSS) persistente

INCIBE ha coordinado la publicación de una vulnerabilidad en Wocu Monitoring, con el código interno INCIBE-2022-0593, que ha sido descubierta por David Cámara Galindo, de Telefónica Tech.

A esta vulnerabilidad se le ha asignado el código CVE-2021-4035. Se ha calculado una puntuación base CVSS v3.1 de 6.8, siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H.

Avisos técnicos - Febrero 2022

TCMAN GIM es vulnerable a Cross-Site Scripting (XSS)

El INCIBE ha coordinado la publicación de una vulnerabilidad en TCMAN GIM, con el código interno INCIBE-2022-0596, que ha sido descubierta por Pablo Arias Rodríguez y Jorge Alberto Palma Reyes, investigadores de Red Team del CSIRT-CV.

A esta vulnerabilidad se le ha asignado el código CVE-2021-4046. Se ha calculado una puntuación base CVSS v3.1 de 6,5, siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L.

Actualizaciones de seguridad de Microsoft de febrero de 2022

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de febrero, y que incluye toda la información comprendida entre el día 12/01/2022 y el día 08/02/2022 con la publicación del boletín de este mes, consta de 94 vulnerabilidades (con CVE asignado) y 0 avisos de seguridad (con ADV asignado), todos ellos calificados como: 51 de severidad alta, 2 de severidad media y 41 sin severidad asignada.

Avisos técnicos - Febrero 2022

Actualización de seguridad de SAP de febrero de 2022

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

Avisos técnicos - Febrero 2022

Vulnerabilidad de ejecución remota de código en Tapo C200 de TP-LINK

INCIBE ha coordinado la publicación de una vulnerabilidad en TP-Link Tapo C200, con el código interno INCIBE-2021-0601, que ha sido descubierta por Víctor Fresco Perales.

A esta vulnerabilidad se le ha asignado el código CVE-2021-4045. Se ha calculado una puntuación base CVSS v3.1 de 9,8, siendo el cálculo del CVSS el siguiente:
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Múltiples vulnerabilidades en productos VMware

Los investigadores Wei de Kunlun Lab, junto con Dimitri Di Cristofaro y Przemek Reszke de SECFORCE LTD, han reportado 6 vulnerabilidades, 5 de severidad alta y 1 media, aunque la combinación de dichas vulnerabilidades podría resultar en una severidad crítica.

Múltiples vulnerabilidades en productos de TIBCO

TIBCO ha reportado 3 vulnerabilidades: 2 de severidad crítica y 1 de severidad alta por las que un atacante no autenticado con acceso a la red podría ejecutar métodos de la API en el sistema afectado y obtener nombres y contraseñas de los usuarios.

Múltiples vulnerabilidades en el core de Drupal

Se han publicado dos vulnerabilidades de severidad media que podrían afectar al core de Drupal.

Avisos técnicos - Febrero 2022

Múltiples vulnerabilidades en productos de GitLab

GitLab ha publicado 7 vulnerabilidades: 1 de severidad crítica, 5 de severidad media y 1 de severidad baja, por las que un atacante podría acceder al token de registro, añadir usuarios a grupos a través de una API, acceder a variables de entorno, listar usuarios no autenticados, ejecutar comandos arbitrarios, filtrar credenciales o causar una denegación de servicio.