Hasta el 9 de noviembre

AVISOS TÉCNICOS

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

GRUPO spri TALDEA

cyber zaintza

Autorización incorrecta en Confluence Data Center y Confluence Server de Atalassian

Atlassian ha informado de una vulnerabilidad de severidad crítica que podría ser explotada por un atacante y provocar una perdida significativa de datos.

Avisos técnicos - Hasta el 9 de noviembre

Server-Side Request Forgery en productos Sage

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a Sage XRT Business Exchange DMZ y Proxy Tools, una solución para el intercambio de datos financieros intragrupo y con las entidades financieras, la cual ha sido descubierta por Rafael Pedrero.

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

CVE-2023-4660: CVSS v3.1: 7.5 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | CWE-918.

Avisos técnicos - Hasta el 9 de noviembre

Inyección de comandos en Cisco Firepower Management Center

Javier Ortega Palacios, investigador de Cisco, ha detectado una vulnerabilidad crítica durante unas pruebas internas de seguridad. La explotación de esta vulnerabilidad podría permitir a un atacante, remoto y autenticado, ejecutar comandos de configuración no autorizados en el dispositivo FTD (Firepower Threat Defense) que es gestionado por FMC (Firepower Management Center).

Avisos técnicos - Hasta el 9 de noviembre

Ejecución remota de código en ActiveMQ de Apache

Rapid7 Managed Detección y Respuesta (MDR) ha identificado una explotación sospechosa de una vulnerabilidad crítica en Apache ActiveMQ que podría permitir a un atacante remoto, con acceso a la red, ejecutar comandos de shell arbitrarios.

Avisos técnicos - Hasta el 9 de noviembre

Múltiples vulnerabilidades en ManageEngine Desktop Central

INCIBE ha coordinado la publicación de 3 vulnerabilidades que afectan a ManageEngine Desktop Central 9.1.0, las cuales han sido descubiertas por Rafael Pedrero.

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:

CVE-2023-4767: CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-93.
CVE-2023-4768: CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-93.
CVE-2023-4769: CVSS v3.1: 6.6 | CVSS: AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H | CWE-918.

Avisos técnicos - Hasta el 9 de noviembre

Múltiples vulnerabilidades en WPN-XM Serverstack

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a WPN-XM Serverstack 0.8.6, las cuales han sido descubiertas por Rafael Pedrero.

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:

CVE-2023-4591: CVSS v3.1: 7.5 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | CWE-829.
CVE-2023-4592: CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-79.

Avisos técnicos - Hasta el 9 de noviembre

Múltiples vulnerabilidades Oday en Microsoft Exchange

Piotr Bazydlo, de la iniciativa Trend Micro Zero Day, ha reportado 4 vulnerabilidades de severidad alta que permite a los atacantes remotos revelar información confidencial y ejecutar código arbitrario sobre las instalaciones afectadas de Microsoft Exchange.

Avisos técnicos - Hasta el 9 de noviembre

Boletín de seguridad de Android de noviembre de 2023

El boletín de Android, relativo a noviembre 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 o provocar una denegación de servicio (DoS).

Avisos técnicos - Hasta el 9 de noviembre

Múltiples vulnerabilidades en chipsets Exynos de Samsung

Daniel Komaromy ha reportado dos vulnerabilidades de severidad alta en diversos procesadores de la gama Exynos.

Avisos técnicos - Hasta el 9 de noviembre

Actualización de seguridad de Android-Noviembre 2023

Google ha publicado las actualizaciones de seguridad de Android y los dispositivos Google Pixel del mes de noviembre de 2023, en donde se corrigen 37 vulnerabilidades de las versiones 10, 11, 12, 13 y 14 del sistema operativo y componentes asociados, abarcando soluciones para fallos de denegación de servicio, elevación de privilegios y divulgación de información. De todas ellas, 5 están calificadas con una severidad crítica y 32 alta.

Avisos técnicos - Hasta el 9 de noviembre

Validación incorrecta de datos de entrada en Lanaccess ONSAFE MonitorHM Web Console

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a Lanaccess ONSAFE MonitorHM 3.7.0, que ha sido descubierta por Petar Alexandrov Nikolov.

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

CVE-2023-6012: CVSS v3.1: 8.3 | CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L | CWE-20.

Avisos técnicos - Hasta el 9 de noviembre

Múltiples vulnerabilidades en PHPMemcachedAdmin

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a PHPMemcachedAdmin, un programa para la administración gráfica autónoma para memcached con fines de supervisión y depuración, las cuales han sido descubiertas por Rafael Pedrero.

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:

CVE-2023-6026: CVSS v3.1: 9.8 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CWE-22.
CVE-2023-6027: CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-79.

Avisos técnicos - Hasta el 9 de noviembre

Vulnerabilidad de elemento de ruta de búsqueda no controlada en 4D y 4D server Windows

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a los ejecutables 4D y 4D server Windows y que ha sido descubierta por Alexander Huaman Jaimes (@zanganox).

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

CVE-2023-4770: CVSS v3.1: 6.5 | CVSS: AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H | CWE-427.

Avisos técnicos - Hasta el 9 de noviembre