Boletín de septiembre de 2020

Avisos Técnicos

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Múltiples vulnerabilidades en Liferay Portal

Fecha de publicación: 01/09/2020

Importancia: Crítica

Recursos afectados:

Liferay Portal, versiones anteriores a 7.3.3.

Descripción:

Liferay Portal ha informado de 3 vulnerabilidades, todas de severidad alta o crítica, de tipo omisión de comprobación de URL y denegación de servicio (DoS).

Solución:

Actualizar a las siguientes versiones:

- para Liferay Portal 7.3, actualizar a Liferay Portal 7.3 CE GA4 (7.3.3) o posterior;
- para Liferay Portal 7.2, su solución está disponible en GitHub;
- para Liferay Portal 7.1, su solución está disponible en GitHub.

Detalle:

- Liferay Portal no decodifica una URL antes de determinar si se debe servir el recurso, lo que podría permitir a un atacante remoto acceder a los recursos de *portlet* restringidos a través de URL con doble codificación. Se ha reservado el identificador CVE-2020-15840 para esta vulnerabilidad.
- Liferay Portal no restringe el tamaño del valor *multipart/form-data* del atributo *enctype* en una petición POST, lo que podría permitir a un usuario autenticado de forma remota realizar ataques de denegación de servicio mediante la carga de archivos grandes. Se ha reservado el identificador CVE-2020-15839 para esta vulnerabilidad.
- El módulo de redireccionamiento en Liferay Portal no limita la cantidad de URL generadas al registrarse un código de error 404, lo que podría permitir a un atacante remoto realizar un ataque de denegación de servicio al enviar solicitudes repetidas de páginas que no existen. Se ha reservado el identificador CVE-2020-24554 para esta vulnerabilidad.

Además de estas vulnerabilidades, Liferay ha informado de otras de menor criticidad. Para más información consulte la página de reporte de vulnerabilidades del fabricante.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad de inyección de código en IBM Spectrum Protect Operations Center

Fecha de publicación: 02/09/2020

Importancia: Crítica

Recursos afectados:

IBM Spectrum Protect Operations Center versiones: desde 8.1.0.000 hasta 8.1.9.xxx y desde 7.1.0.000 hasta 7.1.10.xxx.

Descripción:

Desde IBM se ha informado de una vulnerabilidad provocada por una validación incorrecta de los datos antes de la exportación en IBM Spectrum Protect Operations Center, que puede permitir que un atacante ejecute código arbitrario en el sistema.

Solución:

Se recomienda instalar las siguientes versiones: 8.1.10.000 y 7.1.11.000.

Detalle:

La vulnerabilidad conocida en IBM Spectrum Protect Operations Center afecta a sistemas AIX, Linux y Windows, y puede permitir que un atacante ejecute código arbitrario en el sistema, causado por una validación incorrecta de los datos antes de la exportación. Se ha reservado el identificador CVE-2020-4693 para esta vulnerabilidad

Etiquetas: Actualización, IBM, Linux, Vulnerabilidad, Windows

---

Validación de entrada incorrecta en Cisco Jabber para Windows

Fecha de publicación: 03/09/2020

Importancia: Crítica

Recursos afectados:

Cisco Jabber para Windows, versiones:

- 12.1;
- 12.5;
- 12.6;
- 12.7;
- 12.8;
- 12.9.

Descripción:

Olav Sortland Thoresen, de Watchcom, ha descubierto una vulnerabilidad, de severidad crítica, de tipo validación de entrada incorrecta, que afecta a Cisco Jabber para Windows.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de Software de Cisco. Para información más detallada, consulte la sección *Fixed Releases* del aviso de Cisco.

Detalle:

Un atacante remoto, autenticado, podría aprovechar esta vulnerabilidad enviando mensajes de XMPP, especialmente diseñados, al *software* afectado. Esto causaría que la aplicación ejecutase programas arbitrarios con los privilegios de la cuenta de usuario que ejecuta el *software* cliente Cisco Jabber, lo que podría generar una ejecución de código arbitrario (RCE). Se ha reservado el identificador CVE-2020-3495 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Comunicaciones, Vulnerabilidad, Windows

---

Actualización de seguridad de SAP de septiembre de 2020

Fecha de publicación: 08/09/2020

Importancia: Crítica

Recursos afectados:

- SAP Solution Manager (User Experience Monitoring), versión 7.2;
- SAP Business Client, versión 6.5;
- SAP Marketing (Mobile Channel Servlet), versiones 130, 140 y 150;
- SAP NetWeaver (ABAP Server) and ABAP Platform, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754 y 755;
- SAP Netweaver AS ABAP, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753 y 754;
- BANKING SERVICES FROM SAP 9.0 (Bank Analyzer), versión 500;
- S/4HANA FIN PROD SUBLDGR, versión 100;
- SAP Commerce, versiones 6.7, 1808, 1811, 1905 y 2005;
- SAP NetWeaver AS ABAP (BSP Test Application), versiones 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754 y755;
- SAPUI5 (UISAPUI5_JAVA), versión 7.50;
- SAPUI5 (SAP_UI), versiones 750, 751, 752, 753, 754 y 755;
- SAPUI5 (UI_700), versión 200;
- SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP NetWeaver (Knowledge Management), versiones 7.30, 7.31, 7.40 y 7.50;
- SAP Business Objects Business Intelligence Platform (BI Workspace), versiones 4.1 y 4.2;
- SAPFiori (Launchpad), versiones 750, 752, 753, 754 y 755;
- SAP 3D Visual Enterprise Viewer, versión 9;
- SAP Adaptive Server Enterprise, versiones 15.7, 16.0.

Descripción:

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

Solución:

Visitar el portal de soporte de SAP e instalar las actualizaciones o los parches necesarios, según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 10 notas de seguridad y 6 actualizaciones, siendo 4 de ellas de severidad crítica, 2 altas, 9 medias y 1 baja.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 2 vulnerabilidades de inyección de código,
- 7 vulnerabilidades de *Cross-Site Scripting*,
- 1 vulnerabilidad de control de acceso inadecuado,
- 1 vulnerabilidad de falta de comprobación de autorización,
- 38 vulnerabilidades de inadecuada validación de los datos de entrada;
- 1 vulnerabilidad de falta de comprobación de autenticación,
- 6 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Vulnerabilidad en Mobile Channel Servlet podría permitir a un atacante autentificado invocar ciertas funciones que están restringidas para realizar tareas relacionadas con los datos de contacto e interacción. Se ha asignado el identificador CVE-2020-6320 para esta vulnerabilidad.
- Vulnerabilidad de inyección de código en las plataformas SAP NetWeaver AS ABAP y SAP ABAP podrían permitir a un atacante tomar el control completo de la aplicación, incluyendo la visualización, modificación o eliminación de datos mediante la inyección de código en la zona de memoria que posteriormente es ejecutada por la aplicación. También se puede utilizar para causar un fallo general en la aplicación que provoque su finalización. Se ha asignado el identificador CVE-2020-6318 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores: CVE-2020-6207, CVE-2020-6296, CVE-2020-6275, CVE-2020-6311, CVE-2020-6302, CVE-2020-6324, CVE-2020-11022, CVE-2020-11023, CVE-2020-6282, CVE-2020-6326, CVE-2020-6313, CVE-2020-6325, CVE-2020-6312, CVE-2020-6288, CVE-2020-6283, CVE-2020-6322, CVE-2020-6327, CVE-2020-6330, CVE-2020-6333, CVE-2020-6346, CVE-2020-6350, CVE-2020-6339, CVE-2020-6356, CVE-2020-6360, CVE-2020-6361, CVE-2020-6328, CVE-2020-6341, CVE-2020-6343, CVE-2020-6351, CVE-2020-6352, CVE-2020-6358, CVE-2020-6348, CVE-2020-6349, CVE-2020-6347, CVE-2020-6337, CVE-2020-6331, CVE-2020-6332, CVE-2020-6335, CVE-2020-6314, CVE-2020-6359, CVE-2020-6344, CVE-2020-6340, CVE-2020-6336, CVE-2020-6338, CVE-2020-6334, CVE-2020-6353, CVE-2020-6329, CVE-2020-6354, CVE-2020-6345, CVE-2020-6355, CVE-2020-6342, CVE-2020-6321, CVE-2020-6357 y CVE-2020-6317.

Etiquetas: Actualización, SAP, Vulnerabilidad

Boletín de seguridad de Microsoft de septiembre de 2020

Fecha de publicación: 09/09/2020

Importancia: Crítica

Recursos afectados:

- Microsoft Windows,
- Microsoft Edge (EdgeHTML-based),
- Microsoft Edge (Chromium-based),

- Microsoft ChakraCore,
- Internet Explorer,
- SQL Server,
- Microsoft JET Database Engine,
- Microsoft Office and Microsoft Office Services and Web Apps,
- Microsoft Dynamics,
- Visual Studio,
- Microsoft Exchange Server,
- SQL Server,
- ASP.NET,
- Microsoft OneDrive,
- Azure DevOps.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de septiembre, consta de 127 vulnerabilidades, 23 clasificadas como críticas y 104 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de Microsoft se informa de los distintos métodos para llevar a cabo dichas actualizaciones.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- denegación de servicio,
- escalada de privilegios,
- divulgación de información,
- ejecución remota de código,
- elusión de las medidas de seguridad,
- suplantación de identidad (spoofing),
- manipulación (tampering).

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Múltiples vulnerabilidades en Clous Pak System de IBM

Fecha de publicación: 10/09/2020

Importancia: Crítica

Recursos afectados:

IBM Cloud Pak System, versiones V2.3.0.1, V2.3.1.1.

Descripción:

IBM ha publicado varias vulnerabilidades de severidad crítica en IBM Cloud Pak System que podrían permitir a un atacante ejecutar código remoto en el sistema.

Solución:

Actualizar a IBM Cloud Pak System V2.3.2.0.

Detalle:

FasterXML jackson-databind maneja inapropiadamente la interacción entre la serialización de gadgets y el tipeo, relacionada a br.com.anteros.dbcp.AnterosDBCPConfig (también se conoce como anteros-core), lo que podría permitir a un atacante remoto ejecutar código arbitrario mediante el envío de entradas especialmente diseñadas. Se ha asignado el identificador CVE-2020-24616 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Desbordamiento de búfer en PAN-OS de Paloalto

Fecha de publicación: 10/09/2020

Importancia: Crítica

Recursos afectados:

- PAN-OS 9.1, versiones anteriores a la 9.1.3;
- PAN-OS 9.0, versiones anteriores a la 9.0.9;
- PAN-OS 8.1, versiones anteriores a la 8.1.15;
- PAN-OS 8.0, todas las versiones.

Descripción:

Paloalto ha publicado una vulnerabilidad, de severidad crítica, en PAN-OS que podría permitir a un atacante, no autenticado, ejecutar código arbitrario con permisos de root.

Solución:

Actualizar a las versiones PAN-OS 8.1.15, PAN-OS 9.0.9, PAN-OS 9.1.3 y posteriores.

Las versiones PAN-OS 7.1 y 8.0, se encuentran discontinuadas y no contarán con ninguna actualización.

Detalle:

Una vulnerabilidad de desbordamiento de búfer podría permitir a un atacante, no autenticado, ejecutar código arbitrario con permisos de root, mediante el envío de peticiones maliciosas a Captive Portal o al interfaz Multi-Factor Authentication. Se ha asignado el identificador CVE-2020-2040 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Escalada de privilegios en productos Intel

Fecha de publicación: 10/09/2020

Importancia: Crítica

Recursos afectados:

Intel® AMT e Intel® ISM, versiones anteriores a la 11.8.79, 11.12.79, 11.22.79, 12.0.68 y 14.0.39.

Descripción:

Intel ha publicado una vulnerabilidad de severidad crítica que podría permitir a un atacante local, no autenticado, la escalada de privilegios.

Solución:

Actualizar a la última versión disponible.

Detalle:

Las restricciones inadecuadas en el búfer podrían permitir a un atacante local, no autenticado, la escalada de privilegios, mediante el acceso a la red. Se ha reservado el identificador CVE-2020-8758 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidades en el core de Drupal

Fecha de publicación: 17/09/2020

Importancia: Alta

Recursos afectados:

Versiones anteriores a:

- 9.0.6;
- 8.9.6;
- 8.8.10;
- 7.73.

Descripción:

Se han publicado 5 vulnerabilidades en el *core* de Drupal, una de severidad alta y el resto medias, de tipos XSS, omisión de autenticación y divulgación de información.

Solución:

Actualizar a las versiones 9.0.6, 8.9.6, 8.8.10 o 7.73.

Las versiones de Drupal 8 anteriores a 8.8.x están al final de su vida útil y ya no reciben cobertura de seguridad. Los portales en versiones 8.7.x o anterior deberán actualizarse a 8.8.10.

Detalle:

La vulnerabilidad de severidad más alta es de tipo XSS reflejado, y podría permitir que un atacante aprovechara la forma en que se representa HTML para los formularios afectados. Se ha reservado el identificador CVE-2020-13668 para esta vulnerabilidad.

Para el resto de vulnerabilidades con menor criticidad se han reservado los identificadores: CVE-2020-13666, CVE-2020-13667, CVE-2020-13669 y CVE-2020-13670.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos Netgear

Fecha de publicación: 18/09/2020

Importancia: Crítica

Recursos afectados:

- CBR40, versiones de firmware anteriores a la 2.5.0.10;
- RBK752, versiones de firmware anteriores a la 3.2.15.25;
- RBR750, versiones de firmware anteriores a la 3.2.15.25;
- RBS750, versiones de firmware anteriores a la 3.2.15.25;
- RBK852, versiones de firmware anteriores a la 3.2.16.6;
- RBR850, versiones de firmware anteriores a la 3.2.16.6;
- RBS850, versiones de firmware anteriores a la 3.2.16.6;
- D6200, versiones de firmware anteriores a la 1.1.00.40;
- D7000, versiones de firmware anteriores a la 1.0.1.78;
- R6020, versiones de firmware anteriores a la 1.0.0.42;
- R6080, versiones de firmware anteriores a la 1.0.0.42;
- R6050, versiones de firmware anteriores a la 1.0.1.26;
- JR6150, versiones de firmware anteriores a la 1.0.1.26;
- R6120, versiones de firmware anteriores a la 1.0.0.66;
- R6220, versiones de firmware anteriores a la 1.1.0.100;
- R6260, versiones de firmware anteriores a la 1.1.0.66;
- R6700v2, versiones de firmware anteriores a la 1.2.0.62;
- R6800, versiones de firmware anteriores a la 1.2.0.62;
- R6900v2, versiones de firmware anteriores a la 1.2.0.62;
- AC2100, versiones de firmware anteriores a la 1.2.0.62;
- AC2400, versiones de firmware anteriores a la 1.2.0.62;
- AC2600, versiones de firmware anteriores a la 1.2.0.62;
- R7450, versiones de firmware anteriores a la 1.2.0.62;
- WNR2020, versiones de firmware anteriores a la 1.1.0.62;
- JGS516PE, versiones de firmware anteriores a la 2.6.0.43;
- RAX40, versiones de firmware anteriores a la 1.0.3.80.

Descripción:

Netgear ha publicado múltiples vulnerabilidades de severidad crítica que afectan a algunos de sus productos.

Solución:

Actualizar a la última versión de firmware disponible, para ello:

- Visite la página de soporte de NETGEAR.
- Introduzca el número de su modelo en el cuadro de búsqueda y selecciónelo en el menú desplegable.
- También puede seleccionar una categoría de producto concreto para buscar su modelo.
- Haga clic en descargas.
- En versiones actuales, seleccione la descarga cuyo título comience con versión del firmware.
- Haga clic en descargar.
- Siga las instrucciones del manual de usuario, las notas de la versión del firmware o la página de asistencia técnica del producto para instalar el nuevo firmware.

Detalle:

Los tipos de vulnerabilidades se corresponden con:

- 3 vulnerabilidades de omisión de autenticación;
- 1 vulnerabilidad de falta de control de acceso de nivel de función;
- 2 vulnerabilidades de inyección de comandos previa a la autenticación;
- 6 vulnerabilidades de divulgación de las credenciales de administrador;
- 2 vulnerabilidades de divulgación de información confidencial;
- 1 vulnerabilidad de configuración inadecuada.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en HPE PPU UCS Meter

Fecha de publicación: 18/09/2020

Importancia: Crítica

Recursos afectados:

HPE Pay Per Use (PPU) Utility Computing Service (UCS) Meter, versión 1.9.

Descripción:

El investigador conocido como "rgod", en colaboración con Trend Micro de ZDI, ha reportado 3 vulnerabilidades, 1 de severidad crítica y 2 altas, de tipo ejecución remota de código (RCE) y divulgación de información.

Solución:

HPE ha discontinuado el programa de desarrollo del producto afectado y la descarga del mismo ha sido eliminada de *My HPE*

Software Center, por lo que se recomienda borrar este producto al quedar obsoleto.

Dada la naturaleza de las vulnerabilidades, la única estrategia de mitigación consiste en restringir la interacción con la aplicación.

Detalle:

- Un atacante remoto, no autenticado, podría ejecutar código arbitrario, en el contexto del sistema, en instalaciones afectadas de HPE PPU UCS Meter, debido a una falta de validación adecuada en la clase *ReceiverServlet*. Se ha asignado el identificador CVE-2020-24626 para esta vulnerabilidad.
- Un atacante remoto, no autenticado, podría divulgar información, en el contexto del sistema, en instalaciones afectadas de HPE PPU UCS Meter, debido a una falta de validación adecuada en la clase *DownloadServlet*. Se ha asignado el identificador CVE-2020-24624 para esta vulnerabilidad.
- Un atacante remoto, no autenticado, podría divulgar información, en el contexto del sistema, en instalaciones afectadas de HPE PPU UCS Meter, debido a una falta de validación adecuada en la clase *ReceiverServlet*. Se ha asignado el identificador CVE-2020-24625 para esta vulnerabilidad.

Etiquetas: HP, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 22/09/2020

Importancia: Alta

Recursos afectados:

- Desde la versión 3.9, hasta la versión 3.9.1;
- desde la versión 3.8, hasta la versión 3.8.4;
- desde la versión 3.7, hasta la versión 3.7.7;
- desde la versión 3.5, hasta la versión 3.5.13;
- versiones anteriores no compatibles.

Descripción:

Varios investigadores han reportado 5 vulnerabilidades, 3 con severidad alta y 2 bajas, de tipo XSS almacenado, XSS reflejado, escalada de privilegios, denegación de servicio (DoS) y falta de sanitización de código JavaScript.

Solución:

Moodle ha publicado diversas actualizaciones, en función de la versión afectada:

- 3.9.2;
- 3.8.5;
- 3.7.8;
- 3.5.14.

Detalle:

- El campo de perfil del usuario *moodlenetprofile* no valida suficientemente los datos introducidos para evitar el riesgo de sufrir un ataque XSS almacenado. Se ha asignado el identificador CVE-2020-25627 para esta vulnerabilidad.
- El filtro en el registro de tareas de administración no valida suficientemente los datos introducidos para evitar el riesgo de sufrir un ataque XSS reflejado. Se ha asignado el identificador CVE-2020-25628 para esta vulnerabilidad.
- El tamaño descomprimido de los archivos *zip* no se comprobó en relación a la cuota de usuario disponible antes de descomprimirlos, lo que podría generar una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2020-25630 para esta vulnerabilidad.

Para el resto de vulnerabilidades con severidad baja, se han asignado los identificadores: CVE-2020-25629 y CVE-2020-25631.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en IBM Tivoli Monitoring

Fecha de publicación: 24/09/2020

Importancia: Crítica

Recursos afectados:

IBM Tivoli Monitoring, versión 6.3.0, Fix Pack 7, Service Pack 5.

Descripción:

IBM ha publicado 4 vulnerabilidades, 3 de severidad media y 1 crítica, en IHS server y en WebSphere Application Server, productos que a su vez están incluidos en IBM Tivoli Monitoring (ITM).

Solución:

Aplicar el parche 6.X.X-TIV-ITM_TEPS_EWAS-IHS_ALL_8.55.17.01 VRMF 6.3.0.x.

Detalle:

- IBM WebSphere Application Server podría permitir a un atacante remoto ejecutar código arbitrario en el sistema a través de una secuencia de objetos serializados especialmente diseñada. Se ha asignado el identificador CVE-2020-4450 para esta vulnerabilidad de severidad crítica.
- La representación de datos inapropiada en IBM WebSphere Application Server, podría permitir a un atacante remoto obtener información confidencial. Se ha asignado el identificador CVE-2019-4670 para esta vulnerabilidad de severidad media.
- Un atacante autenticado podría crear un nombre de archivo diseñado con fines maliciosos que sería interpretado inapropiadamente como contenido *jsp* y ejecutado. Se ha asignado el identificador CVE-2020-4163 para esta vulnerabilidad de severidad media.
- La inadecuada eliminación de las propiedades de las clases en Apache Commons Beanutils podría permitir a un atacante remoto el acceso no autorizado al sistema. Se ha asignado el identificador CVE-2019-10086 para esta vulnerabilidad de severidad media.

Etiquetas: Actualización, IBM, Vulnerabilidad