Boletín de Julio de 2018

Avisos Técnicos

Múltiples vulnerabilidades en Db2 de IBM

Fecha de publicación: 09/07/2018

Importancia: Alta

Recursos afectados:

Versiones de IBM Db2:

- V9.7.
- V10.1.
- V10.5.
- V11.1.

Descripción:

IBM ha detectado 3 vulnerabilidades de criticidad alta en Db2 que podría permitir a un atacante local elevación de privilegios y ejecución arbitraria de código

Solución:

IBM ha puesto a disposición de los usuarios actualizaciones que solucionan las vulnerabilidades en función de la versión y plataforma de Db2 afectada.

Las actualizaciones correspondientes de Db2 son:

- V9.7 FP11 para versiones V9.7.
- V10.1 FP6 para versiones V10.1.
- V10.5 FP9 para V10.5.
- V11.1.3 iFix001 para V11.1.3.

Los enlaces de descargas están disponibles en la sección Referencias.

Detalle:

- La carga de librerías en Db2 a través de rutas potencialmente no confiables podrían permitir a un usuario, con bajos privilegios en el sistema, acceso completo a la cuenta de instancia Db2. Se ha reservado el identificador CVE-2018-1487 para esta vulnerabilidad.
- Múltiples vulnerabilidades en Db2 Administration Server de Windows podrían permitir a un usuario local ejecutar código arbitrario. Se ha reservado el identificador CVE-2018-1458 para esta vulnerabilidad.
- La herramienta db2support está afectada por una vulnerabilidad de formato de cadena, la cual podría permitir a un usuario local ejecutar código arbitrario. Se ha reservado el identificador CVE-2018-1566 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Boletín de seguridad de Microsoft de julio de 2018

Fecha de publicación: 11/07/2018

Importancia: Crítica

Recursos afectados:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows

- Microsoft Office, Microsoft Office Services y Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- ASP.NET
- Microsoft Research JavaScript Cryptography Library
- Skype for Business and Microsoft Lync
- Visual Studio
- Microsoft Wireless Display Adapter V2 Software
- PowerShell Editor Services
- PowerShell Extension para Visual Studio Code
- Web Customizations para Active Directory Federation Services

Descripción:

La publicación mensual de actualizaciones de seguridad de Microsoft de este mes consta de 50 vulnerabilidades, 17 clasificadas como críticas y 33 como importantes, siendo el resto de las vulnerabilidades publicadas en el boletín de severidad media o baja.

Solución:

Instalar la actualización correspondiente. En la página de información de instalación de las actualizaciones de seguridad, se informa de los distintos métodos de actualización.

Detalle:

En el boletín de actualizaciones de seguridad correspondiente al mes de julio se han publicado vulnerabilidades de seguridad de los siguientes tipos:

- Denegación de serivicio.
- Elevación de privilegios.
- Revelación de información.
- Ejecución remota de código.
- Evasión de seguridad.
- Suplantación.

Etiquetas: Actualización, Microsoft, Vulnerabilidad

Múltiples vulnerabilidades en productos de Intel

Fecha de publicación: 11/07/2018

Importancia: Alta

Recursos afectados:

- 4ª, 5ª, 6ª y 7ª generación de procesadores Intel Core
- Productos con firmware basado en Tiancore
- Firmware BMC en placas de servidor, módulos de cómputo y sistemas de Intel
- Distribución de Python de Intel
- Intel CSME (Converged Security Management Engine)
- Intel Active Management Technology

Descripción:

Intel ha publicado siete vulnerabilidades, todas ellas de severidad alta, que afectan a varios de sus productos.

Solución:

Visite el sitio de Intel de soporte y descargas para obtener el parche o la actualización correspondiente a su producto.

Detalle:

Un atacante podría llegar a realizar las siguientes acciones mediante la explotación de las vulnerabilidades descritas en este aviso:

- Revelación de información
- Escalada de privilegios
- Denegación de servicio

Se han reservado los siguientes identificadores: CVE-2017-5704, CVE-2018-3651, CVE-2018-3650, CVE-2018-3627, CVE-2018-3628, CVE-2018-3629 y CVE-2018-3632 para estas vulnerabilidades.

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Actualización de seguridad de SAP de julio 2018

Fecha de publicación: 11/07/2018

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5
- SAP Internet Sales, versiones 7.30,7.31, 7.32, 7.33 y 7.54
- SAP Business Objects, versiones 4.0 a 4.10, 4.20 a 4.30
- SAP Crystal Reports, versión para Visual Studio .NET, versión 2010
- AP R/3 Enterprise Retail, versión EHP6
- SAP CrystalReports versión para Visual Studio .NET, version 2010
- SAP BusinessObjects Business Intelligence Suite, versiones 4.10 y 4.20

- SAP Business Objects Enterprise, versiones 4.0 y 4.1
- SAP Gateway, versiones SAP KERNEL 32 NUC, SAP KERNEL 32 Unicode, SAP KERNEL 64 NUC, SAP KERNEL 64 Unicode 7.21, 7.21EXT, 7.22 y 7.22EXT; SAP KERNEL 7.21, 7.22, 7.45, 7.49 y 7.53
- SAP MaxDB ODBC driver, versiones 7.9.09.07
- SAP Internet Graphics Server (IGS), versiones 7.20, 7.20EXT, 7.45, 7.49 y 7.53
- SAP Dynamic Authorization Management (DAM) de NextLabs (Java Policy Controller), versiones 7.7 y 8.5
- SAP BusinessObjects Business Intelligence (BI Launchpad y Central Management Console), versiones 4.1, 4.2 y 4.3
- Infrastructure for UI add-on for SAP NetWeaver (UI_Infra), SAP UI Implementation for Decoupled Innovations(UI_700): NW 7.00 Implementation, SAP User Interface Technology (SAP_UI), versiones UI_Infra 1.0; SAP_UI 7.4, 7.5, 7.51 y 7.52; UI_700 2.0

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 actualizaciones o parches necesarios según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 16 notas de seguridad de las cuales, 5 son actualizaciones de notas de seguridad publicadas con anterioridad, 1 de ellas de severidad crítica, 2 de de severidad alta y 13 de severidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 3 vulnerabilidades de inyección de código
- 1 vulnerabilidad de divulgación de información
- 3 vulnerabilidades de denegación de servicio
- 2 vulnerabilidades de Cross-Site Scripting
- 1 vulnerabilidad de falta de verifiación de autorización
- 3 vulnerabilidades de otras tipologías

Las vulnerabilidades más relevantes son las siguientes:

- Una vulnerabilidad de ausencia de verificación de autorización en SAP R/3 Enterprise Retail, podría permitir el acceso a un servicio sin ningún procedimiento de autorización y la utilización de la funcionalidad del servicio que tiene acceso restringido. Esto puede llevar a una revelación de información, elevación de privilegios y otros ataques. Se ha reservado el código CVE-2018-2436 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de código en SAP CrystalReports podría permitir la ejecución de comandos con los mismos privilegios del servicio que ejecutó el comando. Es posible acceder a archivos y directorios arbitrarios ubicados en un sistema de archivos de servidor SAP, incluyendo el código fuente de la aplicación, la configuración y los archivos críticos del sistema. Permite obtener información crítica técnica y de negocio almacenada en un sistema SAP vulnerable. Se ha reservado el identificador CVE-2018-2427 para esta vulnerabilidad.
- Una vulnerabilidad de Cross-Site Scripting en SAP CrystalReports podría permitir a un atacante inyectar un script malicioso en una página, almacenándolo permanentemente en el cuerpo de la página, de esta manera el usuario es atacado sin realizar ninguna acción. El script malicioso puede proporcionar acceso a todas las cookies, tokens de sesión y otra información crítica almacenada por el navegador y utilizada para la interacción con un sitio. El atacante puede acceder a la sesión del usuario y aprender información crítica para el negocio y en algunos casos es posible tener control sobre ella. XSS puede ser utilizado para la modificación no autorizada del contenido del sitio mostrado. Se ha reservado el código CVE-2018-2431 para esta vulnerabilidad.

Etiquetas: Actualización, SAP, Vulnerabilidad

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 12/07/2018

Importancia: Crítica

Recursos afectados:

- IBM Content Navigator 2.0.3.8
- IBM Content Navigator 3.0.2
- IBM Content Navigator 3.0.3
- IBM Security Identity Governance and Intelligence (IGI) versiones: 5.2, 5.2.1, 5.2.2, 5.2.2.1, 5.2.3, 5.2.3.1, 5.2.3.2

Descripción:

IBM ha detectado 3 vulnerabilidades, una de severidad crítica y dos de severidad alta. Donde un atacante remoto podría obtener información sensible, consumir recursos de memoria, deshabilitar el gestor de seguridad y elevación de sus privilegios.

Solución:

IBM ha publicado diversas actualizaciones para solventar las vulnerabilidades en función del producto afectado y su versión.

- IBM Security Identity Governance and Intelligence:
  - Actualizar a la versión 5.2.4.0
- IBM Content Navigator:
  - Para la versión 2.0.3.8 descargar la actualización 2.0.3 FP8 LA 19 en Fix Central.
  - Para la versión 3.0.2 descargar la actualización 3.0.2 LA 06 en Fix Central.
  - Para la versión 3.0.3 descargar la actualización 3.0.3-iFix004 FixCentral.

Detalle:

- IBM Content Navigator tiene una vulnerabilidad del tipo XXE a la hora de procesar datos XML, un atacante podría obtener información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2018-1364 para esta vulnerabilidad.
- Una falla en el verificador de clases en IBM J9 VM podría permitir que código no fiable deshabilite el gestor de seguridad y elevación de sus privilegios. Se ha reservado el identificador CVE-2017-1376 para esta vulnerabilidad.
- IBM Security Identity Governance Virtual Appliance tiene una vulnerabilidad del tipo XXE a la hora de procesar datos XML, un atacante remoto podría obtener información sensible o consumir recursos de memoria. Se ha reservado el identificador CVE-2017-1472 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 12/07/2018

Importancia: Alta

Recursos afectados:

- Cisco Virtualized Packet Core-Single Instance (VPC-SI)
- Cisco Virtualized Packet Core-Distributed Instance (VPC-DI)
- Cisco Ultra Packet Core (UPC)
- IP Phone 6800 Series con Multiplatform Firmware
- IP Phone 7800 Series con Multiplatform Firmware
- IP Phone 8800 Series con Multiplatform Firmware

Descripción:

Se han publicado varias vulnerabilidades que afectan a productos Cisco, que podrían permitir la ejecución remota de código en el servidor web de Cisco IP Phone series 6800, 7800 y 8800 o una condición de denegación de servicio en productos con StarOS.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde: Panel de descarga de Software Cisco.

Detalle:

- Una vulnerabilidad en la lógica de reensamblado de paquetes IPv4 fragmentados de Cisco StarOS, podría permitir a un atacante remoto no autenticado el reinicio del proceso npusim mediante el envío de un paquete IPv4 especialmente diseñado, resultando en una condición de denegación de servicio. Se ha reservado el identificador CVE-2018-0369 para esta vulnerabilidad
- Una incorrecta validación en los datos de entrada, podría permitir a un atacante ejecutar código remoto desde el interfaz de usuario de Cisco IP Phone, series 6800, 7800 y 8800. Se ha reservado el identificador CVE-2018-0341 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de Juniper

Fecha de publicación: 12/07/2018

Importancia: Crítica

Recursos afectados:

- Junos OS, versiones: 12.1X46, 12.3, 12.3X48, 14.1X53, 15.1X49, 15.1, 15.1F5, 15.1F6, 15.1F7, 16.1, 16.1X65, 17.2X75, 17.3, 17.4
- Plataformas Junos OS con MPC7/8/9 o PTX-FPC3 (FPC-P1, FPC-P2) instalado y PTX1K 15.1, 15.1F, 16.1, 16.1X65, 16.2, 17.1, 17.2, 17.2X75, 17.3 y 17.4
- Contrail Service Orchestration versión 4.0.0
- Junos Space versiones anteriores a 18.1R1

Descripción:

Juniper ha publicado varios boletines de seguridad en los que se describen múltiples vulnerabilidades en diversos productos, donde 5 son de severidad crítica y 10 de severidad alta.

Solución:

Nuevas versiones de software, parches y actualizaciones. Están disponibles en https://www.juniper.net/support/downloads/.

Detalle:

Múltiples vulnerabilidades afectan a varios productos de Juniper. Un atacante podría llegar a realizar las siguientes acciones sobre los productos afectados:

- Control total.
- Producción de una condición de denegación de servicio.
- Ejecución remota de código.
- Evasión de autenticación.
- Revelación no autorizada de información.
- Acceso no autorizado a ciertos servicios

Se han asignado los siguientes identificadores para las vulnerabilidades descritas: CVE-2018-0024, CVE-2018-10635, CVE-2018-0027, CVE-2018-0030, CVE-2018-0032, CVE-2018-0037, CVE-2017-3145, CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2663, CVE-2018-2678, CVE-2017-12613, CVE-2017-10198, 2017-10281, CVE-2017-10295, CVE-2017-10345, CVE-2017-10355, CVE-2017-10356, CVE-2017-10388, CVE-2017-15896, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en el cliente BIG-IP APM para Linux y Mac OS X

Fecha de publicación: 13/07/2018

Importancia: Alta

Recursos afectados:

- BIG-IP (APM) versiones desde la 11.5.1 hasta la 11.5.6, desde la 12.1.0 hasta la 12.1.3 y desde la 13.0.0 hasta la 13.1.0
- Clientes BIG-IP APM con versiones desde la 7.1.5 hasta la 7.1.6.1
- Clientes BIG-IP Edge con versiones desde la 7101 hasta la 7150

Descripción:

F5 ha descubierto una vulnerabilidad de criticidad alta que podría permitir a un atacante local sin privilegios en el sistema la obtención de información sensible, manipulación de datos o la interrupción el servicio.

Solución:

F5 ha publicado la actualización 7.1.7 para solucionar la vulnerabildiad en los clientes BIG-IP APM.

Aún no existe solución para BIG-IP (APM) ni para clientes BIG-IP Edge.

Detalle:

- El componente svpn en el cliente BIG-IP APM se ejecuta a través de procesos con privilegios, lo que podría permitir a un atacante local en el sistema adquirir privilegios de súper usuario en el equipo. Se ha reservado el identificador CVE-2018-5529 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Lectura fuera de límites en VMware Tools

Fecha de publicación: 16/07/2018

Importancia: Alta

Recursos afectados:

- VMware Tools 10.x y anteriores

Descripción:

El investigador Anurudh ha informado a VMware de una vulnerabilidad de severidad alta que podría permitir a un atacante la lectura de memoria fuera de límites.

Solución:

VMware ha publicado la versión 10.3.0 de las tools que soluciona la vulnerabilidad. Se debe instalar la versión nueva de las tools en todas las máquinas virtuales Windows para eliminar la vulnerabilidad.

Detalle:

En máquinas virtuales Windows que tengan las tools instaladas con la compartición de ficheros activada, un atacante podría llegar a realizar una lectura fuera de límites, lo que le podría permitir:

- Acceso no autorizado a información
- Escalar privilegios en las máquinas virtuales

Se ha asignado el identificador CVE-2018-6969 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Actualizaciones críticas en Oracle (Julio 2018)

Fecha de publicación: 18/07/2018

Importancia: Crítica

Recursos afectados:

- Agile Recipe Management for Pharmaceuticals, versión 9.3.4
- Enterprise Manager Base Platform, versiónes 12.1.0.5, 13.2.x
- Enterprise Manager for Fusion Middleware, versiónes 12.1.0.5, 13.2.x
- Enterprise Manager for MySQL Database, versiónes 13.2.2.0.0 y anteriores
- Enterprise Manager for Oracle Database, versiónes 12.1.0.8, 13.2.2
- Enterprise Manager for Peoplesoft, versiónes 13.1.1.1, 13.2.1.1
- Enterprise Manager for Virtualization, versiónes 13.2.2, 13.2.3
- Enterprise Manager Ops Center, versiónes 12.2.2, 12.3.3
- FMW Platform, versiónes 12.2.1.2.0, 12.2.1.3.0
- Hardware Management Pack, versión 11.3
- Hyperion Data Relationship Management, versión 11.1.2.4.330
- Hyperion Financial Reporting, versión 11.1.2
- JD Edwards EnterpriseOne Tools, versión 9.2
- JD Edwards World Security, versiónes A9.3, A9.3.1, A9.4
- MICROS 700 Series Tablet, versiónes anteriores a BIOS 0.00.13ORC, anteriores a BIOS 0.01.25ORC
- MICROS Hyheld Terminal, versiónes 2018, yroid 4.4.4 Security Patch Bulletin anteriores a 1 de Febrero
- MICROS Kitchen Display Controller, versiónes anteriores a BIOS 0.00.16ORC
- MICROS Lucas, versiónes 2.9.5.3, 2.9.5.4, 2.9.5.5, 2.9.5.6
- MICROS Relate CRM Software, versiónes 10.8.x, 11.4.x

- MICROS Retail-J, versiónes 10.2.x, 11.0.x, 12.0.x, 12.1.x, 12.1.1.x, 12.1.2.x, 13.1.x
- MICROS Workstation 6, versiónes anteriores a BIOS 1.3.1.0, anteriores a BIOS 1.5.2.0, anteriores a BIOS 2.3.1.0
- MICROS XBR, versiónes 7.0.2, 7.0.4
- MySQL Client, versiónes 5.5.60 y anteriores, 5.6.40 y anteriores, 5.7.22 y anteriores, 8.0.11 y anteriores
- MySQL Connectors, versiónes 5.3.10 y anteriores, 8.0.11 y anteriores
- MySQL Enterprise Monitor, versiónes 3.4.7.4297 y anteriores, 4.0.4.5235 y anteriores, 8.0.0.8131 y anteriores
- MySQL Server, versiónes 5.5.60 y anteriores, 5.6.40 y anteriores, 5.7.22 y anteriores, 8.0.11 y anteriores
- MySQL Workbench, versiónes 6.3.10 y anteriores, 8.0.11 y anteriores
- Oracle Agile Engineering Data Management, versiónes 6.1.3, 6.2.0, 6.2.1
- Oracle Agile PLM, versiónes 9.3.3, 9.3.4, 9.3.5, 9.3.6
- Oracle Agile PLM MCAD Connector, versiónes 3.3, 3.4, 3.5, 3.6
- Oracle Agile Product Lifecycle Management for Process, versión 6.2.0.0
- Oracle API Gateway, versión 11.1.2.4.0
- Oracle Application Testing Suite, versión 10.1
- Oracle AutoVue VueLink Integration, versiónes 21.0.0, 21.0.1
- Oracle Banking Corporate Lending, versiónes 12.3.0, 12.4.0, 12.5.0, 14.0.0, 14.1.0
- Oracle Banking Payments, versiónes 12.2.0, 12.3.0, 12.4.0, 12.5.0, 14.1.0
- Oracle Banking Platform, versiónes 2.6.0, 2.6.1, 2.6.2
- Oracle BI Publisher, versiónes 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0
- Oracle Business Process Management Suite, versiónes 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0
- Oracle Communications Diameter Signaling Router (DSR), versiónes 7.x, 8.x
- Oracle Communications EAGLE LNP Application Processor, versión 10.x
- Oracle Communications Interactive Session Recorder, versiónes 5.x, 6.x
- Oracle Communications Messaging Server, versión 3.x
- Oracle Communications Network Charging y Control, versiónes 4.4.1.5.0, 5.0.0.1.0, 5.0.0.2.0, 5.0.1.0.0, 5.0.2.0.0
- Oracle Communications Policy Management, versión 12.x
- Oracle Communications Session Border Controller, versiónes ECz7.x, ECz8.x
- Oracle Communications User Data Repository, versiónes 10.x, 12.x
- Oracle Database Server, versiónes 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1, 18.2
- Oracle E-Business Suite, versiónes 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7
- Oracle Endeca Information Discovery Studio, versiónes 3.1, 3.2
- Oracle Enterprise Data Quality, versión 12.2.1.3.0
- Oracle Enterprise Repository, versiónes 11.1.1.7.0, 12.1.3.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versiónes 7.3.3.x, 8.0.x
- Oracle Financial Services Behavior Detection Platform, versión 8.0.x
- Oracle Financial Services Funds Transfer Pricing, versiónes 6.1.1, 8.0.x
- Oracle Financial Services Hedge Management y IFRS Valuations, versiónes 8.0.4, 8.0.5
- Oracle Financial Services Loan Loss Forecasting y Provisioning, versiónes 8.0.4, 8.0.5
- Oracle Financial Services Profitability Management, versiónes 6.1.1, 8.0.x
- Oracle Financial Services Revenue Management y Billing, versiónes 2.3.0.2.0, 2.4.0.0.0, 2.4.0.1.0, 2.5.0.1.0, 2.5.0.2.0, 2.5.0.3.0
- Oracle FLEXCUBE Enterprise Limits y Collateral Management, versiónes 12.3.0, 14.0.0, 14.1.0
- Oracle FLEXCUBE Investor Servicing, versiónes 12.0.4, 12.1.0, 12.3.0, 12.4.0
- Oracle FLEXCUBE Universal Banking, versiónes 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0
- Oracle Fusion Middleware, versiónes 12.2.1.2, 12.2.1.3
- Oracle Fusion Middleware MapViewer, versiónes 12.2.1.2, 12.2.1.3
- Oracle Global Lifecycle Management OPatchAuto, versión All
- Oracle Hospitality Cruise Fleet Management System, versión 9.x
- Oracle Hospitality Cruise Shipboard Property Management System, versión 8.x
- Oracle Hospitality Gift y Loyalty, versión 9.0.0
- Oracle Hospitality OPERA 5 Property Services, versión 5.5.x
- Oracle Hospitality Reporting y Analytics, versión 9.0.0
- Oracle Hospitality Simphony, versiónes 2.8, 2.9, 2.10
- Oracle iLearning, versión 6.2
- Oracle Insurance Policy Administration, versiónes 10.0, 10.1, 10.2, 11.0
- Oracle Internet Directory, versión 11.1.1.9.0
- Oracle Java SE, versiónes 6u191, 7u181, 8u172, 10.0.1
- Oracle Java SE Embedded, versión 8u171
- Oracle JDeveloper, versiónes 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0
- Oracle JRockit, versión R28.3.18
- Oracle Outside In Technology, versión 8.5.3
- Oracle Policy Automation, versiónes 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10
- Oracle Policy Automation Connector for Siebel, versión 10.4.6
- Oracle Policy Automation for Mobile Devices, versiónes 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10
- Oracle Retail Back Office, versiónes 14.0, 14.1
- Oracle Retail Bulk Data Integration, versión 16.0
- Oracle Retail Central Office, versiónes 14.0, 14.1
- Oracle Retail Clearance Optimization Engine, versión 14.0.5
- Oracle Retail Convenience y Fuel POS Software, versión 2.1.132
- Oracle Retail Customer Management y Segmentation Foundation, versiónes 16.x, 17.x
- Oracle Retail Financial Integration, versiónes 13.2.x, 14.0.x, 14.1.x, 15.0.x, 16.0.x
- Oracle Retail Integration Bus, versiónes 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.0 14.1.0, 14.0.x, 14.1.x, 15.0, 15.0.x, 16.0, 16.0.x
- Oracle Retail Order Broker, versiónes 5.2, 15.0, 16.0
- Oracle Retail Point-of-Sale, versiónes 14.0, 14.1
- Oracle Retail Point-of-Service, versiónes 14.0, 14.1
- Oracle Retail Predictive Application Server, versión 15.0.3
- Oracle Retail Returns Management, versiónes 14.0, 14.1
- Oracle Retail Service Backbone, versiónes 14.0.x, 14.1.x, 15.0.x, 16.0.x
- Oracle Retail Service Layer, versiónes 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.x
- Oracle Secure Global Desktop, versiónes 5.3, 5.4
- Oracle SOA Suite, versiónes 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0
- Oracle SuperCluster Specific Software, versiónes anteriores a 2.5.0
- Oracle Transportation Management, versiónes 6.2, 6.3.7, 6.4.1
- Oracle Tuxedo, versiónes 12.1.1, 12.1.3, 12.2.2
- Oracle Utilities Framework, versión 4.3.x
- Oracle Utilities Network Management System, versiónes 1.12.x, 2.3.x
- Oracle Utilities Work y Asset Management, versión 1.9.1.2.12
- Oracle VM VirtualBox, versiónes anteriores a 5.2.16
- Oracle WebCenter Portal, versiónes 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0
- Oracle WebLogic Server, versiónes 10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3
- OSS Support Tools, versiónes anteriores a 18.3
- PeopleSoft Enterprise CS Financial Aid, versiónes 9.0, 9.2
- PeopleSoft Enterprise FIN Install, versión 9.2

- PeopleSoft Enterprise HCM Human Resources, versión 9.2
- PeopleSoft Enterprise PeopleTools, versiónes 8.55, 8.56
- PeopleSoft HRMS, versión 9.2
- Primavera P6 Enterprise Project Portfolio Management, versiónes 8.4, 15.x, 16.x, 17.x
- Primavera Unifier, versiónes 16.x, 17.x, 18.x
- Siebel Applications, versión 18.0
- Solaris, versiónes 10, 11.2, 11.3
- Solaris Cluster, versiónes 3.3, 4.3
- Sun ZFS Storage Appliance Kit (AK), versiónes anteriores a 8.7.20
- Tape Library ACSLS, versiónes anteriores a ACSLS 8.4.0-3

Descripción:

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades que afectan a múltiples productos.

Impacto:

Aplicar los parches correspondientes según el/los productos afectados. La información para descargar las actualizaciones puede obtenerse del boletín de seguridad publicado por Oracle.

Solución:

Esta actualización resuelve un total de 334 vulnerabilidades, algunas de las cuales son críticas. El detalle de las vulnerabilidades resueltas se puede consultar en el enlace de Oracle de la sección de Referencias.

Etiquetas: Actualización, Oracle

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 19/07/2018

Importancia: Crítica

Recursos afectados:

- Cisco Policy Suite versiones anteriores a 18.2.0 y 18.1.0
- Cisco Nexus 9000 Series Fabric Switches in ACI Mode
- Cisco SD-WAN Solution versiones anteriores a Release 18.3.0:
  - vBond Orchestrator Software
  - vEdge 100 Series Routers
  - vEdge 1000 Series Routers
  - vEdge 2000 Series Routers
  - vEdge 5000 Series Routers
  - vEdge Cloud Router Platform
  - vManage Network Management Software
  - vSmart Controller Software
- Cisco Webex Meetings Suite
- Cisco Webex Meetings Online
- Cisco Webex Meetings Server

Descripción:

Cisco ha publicado 25 vulnerabilidades en diversos productos, siendo 4 vulnerabilidades de severidad crítica, 9 de severidad alta y 12 de severidad media.

Solución:

Cisco ha puesto a disposición de los usuarios diversas actualizaciones en función del producto afectado. Las actualizaciones que corrigen las vulnerabilidades pueden descargarse desde:

- Panel de descarga de Software Cisco

Detalle:

Las vulnerabilidades de severidad crítica son las siguientes:

- Una vulnerabilidad en Cluster Manager de Cisco Policy Suite podría permitir que un atacante remoto no autenticado inicie sesión en un sistema afectado utilizando la cuenta root, que tiene credenciales de usuario estáticas predeterminadas y no documentadas. Se ha asignado el identificador CVE-2018-0375 para esta vulnerabilidad.
- Una vulnerabilidad en la base de datos de Policy Builder de Cisco Policy Suite podría permitir que un atacante remoto no autenticado se conecte directamente a la base de datos de Policy Builder. Esta vulnerabilidad se debe a la falta de autenticación en la base de datos. Se ha asignado el identificador CVE-2018-0374 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz de Open Systems Gateway initiative (OSGi) de Cisco Policy Suite podría permitir que un atacante remoto no autenticado se conecte directamente a la interfaz OSGi. Esta vulnerabilidad se debe a la falta de autenticación en el servicio OSGi. Se ha asignado el identificador CVE-2018-0377 para esta vulnerabilidad.
- Una vulnerabilidad en la interfaz de Policy Builder de Cisco Policy Suite podría permitir que un atacante remoto no autenticado acceda a la interfaz de Policy Builder. La vulnerabilidad se debe a la falta de autenticación en la interfaz de Policy Builder. Se ha asignado el identificador CVE-2018-0376 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 19/07/2018

Importancia: Alta

Recursos afectados:

Todas las versiones de Jenkins anteriores a la versión 2.133 y Jenkins LTS anteriores a 2.121.2

Descripción:

Se han publicado varias vulnerabilidades en el software de automatización y despliegue de proyectos Jenkins. Un atacante remoto podría aprovechar estas vulnerabilidades para lectura de archivos arbitrarios, restablecimiento de configuraciones, cancelación de trabajos en curso o XSS en la aplicación.

Solución:

Se recomienda actualizar a la versión 2.133 de Jenkins y a la 2.121.2 de Jenkins TLS.

Detalle:

Se han hecho públicas las siguientes vulnerabilidades, de criticidad alta:

- SECURITY-897: Se ha conocido una vulnerabilidad que permitiría a usuarios no autenticados utilizar credenciales de inicio de sesión creadas de forma malintencionada que provoquen que Jenkins mueva el archivo config.xml desde el directorio de inicio de Jenkins. Este archivo de configuración contiene la configuración básica de Jenkins, incluidos los aspectos de seguridad. Si Jenkins se inicia sin este archivo, volverá a los valores predeterminados heredados, y otorgará acceso de administrador a usuarios anónimos.
- SECURITY-914: Se ha detectado una vulnerabilidad de lectura de archivo arbitraria en el framework web de Stapler utilizado por Jenkins permitiendo a los usuarios no autenticados enviar solicitudes HTTP manipuladas y devolviendo el contenido de cualquier archivo del sistema maestro de Jenkins al que tiene acceso el proceso de Jenkins.

También se han hecho públicas otras vulnerabilidades de criticidad media con los identificadores: SECURITY-891, SECURITY-892, SECURITY-944, SECURITY-925 y SECURITY-390.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en en Apache Tomcat

Fecha de publicación: 24/07/2018

Importancia: Alta

Recursos afectados:

- Apache Tomcat versión 9.0.0.M9 to 9.0.9
- Apache Tomcat versión 8.5.0 to 8.5.31
- Apache Tomcat versión 8.0.0.RC1 to 8.0.51
- Apache Tomcat versión 7.0.28 to 7.0.86

Descripción:

Apache Software Foundation ha publicado una actualización de seguridad que corrige varias vulnerabilidades que podrían permitir a un atacante remoto efectuar denegaciones de servicio en el servidor Apache Tomcat u obtener información confidencial del mismo.

Solución:

Se recomienda actualizar a las últimas versiones disponibles 9.0.10, 8.5.32, 8.0.52 y 7.0.90.

Detalle:

Las vulnerabilidades descubiertas incluyen un incorrecto manejo en la descodificación UTF-8 con caracteres suplementarios, algo que puede provocar un bucle infinito en el decodificador, lo que a su vez podría provocar una denegación de servicio. Se ha asignado el identificador CVE-2018-1336 para esta vulnerabilidad.

Además la otra vulnerabilidad descubierta podría permitir la reutilización de sesiones de usuario, al existir un error en el seguimiento de cierres de conexión existentes. Se ha asignado el identificador CVE-2018-1337 para esta vulnerabilidad.

Etiquetas: Actualización, Apache, Vulnerabilidad

Múltiples vulnerabilidades Mbed TLS

Fecha de publicación: 27/07/2018

Importancia: Alta

Recursos afectados:

Mbed TLS versiones 1.2 y superiores, y versiones 2.1, 2.7 y superiores.

Descripción:

Mbed TLS ha anunciado varias vulnerabilidades que permitirán a un atacante la recuperación remota de texto plano cuando se utiliza un cifrado basado en CBC.

Solución:

Se recomienda actualizar a las versiones 2.12.0, 2.7.5 o 2.1.14 o posterior.

Detalle:

Cuando se utiliza un cifrado basado en CBC es posible que un atacante remoto recupere parcialmente un texto sin formato. Para ello el atacante deberá poder capturar e inyectar tráfico de red, y en el caso de utilización de TLS generar múltiples sesiones con el mismo texto, para DTLS con una sesión sería suficiente.

Es posible recuperar parcialmente el texto sin formato de los mensajes que aprovechan los canales laterales de temporización o de caché. Se han asignado a estas vulnerabilidades los identificadores CVE-2018-0497 y CVE-2018-0498.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad