Boletín de enero de 2021

Avisos Técnicos

Vulnerabilidad de credenciales embebidas en múltiples productos de Zyxel

Fecha de publicación: 05/01/2021

Importancia: Alta

Recursos afectados:

Cortafuegos:

- ATP series, versión de firmware ZLD 4.60;
- USG series, versión de firmware ZLD 4.60;
- USG FLEX series, versión de firmware ZLD 4.60;
- VPN series, versión de firmware ZLD 4.60;

Controladores de Punto de Acceso (AP):

- NXC2500, versiones de firmware de la 6.00 a la 6.10;
- NXC5500, versiones de firmware de la 6.00 a la 6.10.

Descripción:

Niels Teusink, de EYE Netherlands, ha reportado a Zyxel una vulnerabilidad de severidad alta de tipo credenciales embebidas.

Solución:

- Para los cortafuegos, está disponible el parche ZLD V4.60 Patch1.
- Para los controladores AP, el fabricante publicará un parche el próximo 8 de enero.

Detalle:

Los productos afectados contienen credenciales embebidas que podrían permitir a un atacante adquirir privilegios de administrador mediante la cuenta de usuario 'zyfwp'. Se ha asignado el identificador CVE-2020-29583 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Dell EMC Avamar Server

Fecha de publicación: 13/01/2021

Importancia: Crítica

Recursos afectados:

- Dell EMC Avamar Server, versiones 19.1, 19.2, 19.3;
- Dell EMC Integrated Data Protection Appliance (IDPA), versiones 2.5 y 2.6.

Descripción:

Dell ha informado de varias vulnerabilidades en EMC Avamar Server que podrían permitir acceso de lectura y escritura no autorizado a los datos de la aplicación, fuga o eliminación de datos de respaldo confidenciales o la ejecución de comandos arbitrarios del sistema operativo.

Solución:

Dell ha publicado los siguientes hotfix para las versiones afectadas:

- EMC Avamar Server 19.1: hotfix 325443;
- EMC Avamar Server 19.2: hotfix 325444;
- EMC Avamar Server 19.3: hotfix 325445;
- EMC Integrated Data Protection Appliance (IDPA) 2.5: hotfix: 325443;
- EMC Integrated Data Protection Appliance (IDPA) 2.6: hotfix: 325445;

Detalle:

Dell ha informado de 2 vulnerabilidades críticas y una alta, siendo las más importantes las siguientes:

- Una vulnerabilidad que permitiría a un atacante remoto no autenticado realizar una inyección SQL en Fitness Analyzer, el backend de la aplicación. Se ha asignado el identificador CVE-2020-29493 para esta vulnerabilidad.
- Una vulnerabilidad de inyección de comandos del sistema operativo en Fitness Analyzer, por lo que un atacante remoto no autenticado podría ejecutar comandos arbitrarios del sistema operativo subyacente de la aplicación. Se ha asignado el identificador CVE-2020-29495 para esta vulnerabilidad.

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Actualización de seguridad de SAP de enero de 2021

Fecha de publicación: 13/01/2021

Importancia: Crítica

Recursos afectados:

- SAP Business Client, versión 6.5;
- SAP Business Warehouse, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755 y 782;
- SAP BW4HANA, versiones 100 y 200;
- SAP NetWeaver AS JAVA, versiones 7.20, 7.30, 7.31, 7.40 y 7.50;
- Automated Note Search Tool (SAP Basis), versiones 7.0, 7.01,7.02, 7.31, 7.4, 7.5, 7.51, 7.52, 7.53 y 7.54;
- SAP NetWeaver AS Java (HTTP Service), versiones 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 y 7.50;
- SAP Commerce Cloud, versiones 1808, 1811, 1905, 2005 y 2011;
- SAP BusinessObjects Business Intelligence platform (Web Intelligence HTML interface), versiones 410 y 420;
- SAP Master Data Governance, versiones 748, 749, 750, 751, 752, 800, 801, 802, 803 y 804;
- SAP NetWeaver AS JAVA (Key Storage Service), versiones 7.10, 7.11, 7.20 ,7.30, 7.31, 7.40 y 7.50;
- SAP GUI FOR WINDOWS, versión 7.60;
- SAP NetWeaver Master Data Management, versiones 7.10, 7.10.750 y 710;
- SAP 3D Visual Enterprise Viewer, versión 9.0;
- SAP Banking Services (Generic Market Data), versiones 400, 450 y 500;
- SAP EPM ADD-IN, versiones 2.8 y 1010;

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.

Para la vulnerabilidad CVE-2021-21465, SAP ha resuelto el problema desactivando el módulo de funciones, por lo que afectará a cualquier aplicación que haga una llamada a este módulo.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 10 notas de seguridad y 7 actualizaciones de notas anteriores, siendo 5 de las nuevas notas de severidad crítica, 1 alta, 10 medias y 1 baja.

Los tipos de vulnerabilidades publicadas se corresponden con los siguientes:

- 2 vulnerabilidades de inyección de código,
- 1 vulnerabilidad de denegación de servicio,
- 3 vulnerabilidades de divulgación de información,
- 4 vulnerabilidades de falta de comprobación de autorización,
- 16 vulnerabilidades de ausencia de validación de entrada,
- 1 vulnerabilidad de inyección SQL,
- 6 vulnerabilidades de otro tipo.

Las notas de seguridad más destacadas se refieren a:

- Una validación de entrada insuficiente en SAP Business Warehouse y en SAP BW4HANA, podría permitir a un atacante, con pocos privilegios, inyectar código malicioso que se almacena de forma persistente como un informe. Este informe podría ser ejecutado posteriormente dando lugar a situaciones con un alto impacto negativo en la confidencialidad, la integridad y la disponibilidad del sistema afectado (y tal vez también de los sistemas conectados). Se ha asignado el identificador CVE-2021-21466 para esta vulnerabilidad.

- Una sanitización inadecuada de los comandos SQL en la interfaz de la base de datos de SAP BW, podría permitir a un atacante ejecutar comandos SQL arbitrarios en la base de datos, lo que podría llevar a un compromiso total del sistema afectado. Se ha asignado el identificador CVE-2021-21465 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores:

CVE-2020-26838, CVE-2020-26820, CVE-2021-21446, CVE-2020-6307, CVE-2020-6224, CVE-2021-21445, CVE-2021-21447, CVE-2020-6256, CVE-2020-26816, CVE-2021-21448, CVE-2021-21469, CVE-2021-21449, CVE-2021-21457, CVE-2021-21458, CVE-2021-21459, CVE-2021-21450, CVE-2021-21451, CVE-2021-21452, CVE-2021-21453, CVE-2021-21454, CVE-2021-21455, CVE-2021-21456, CVE-2021-21460, CVE-2021-21461, CVE-2021-21462, CVE-2021-21463, CVE-2021-21464, CVE-2021-21467 y CVE-2021-21470.

Etiquetas: Actualización, SAP, Vulnerabilidad

Actualizaciones de seguridad de Microsoft de enero de 2021

Fecha de publicación: 13/01/2021

Importancia: Crítica

Recursos afectados:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML-based);
- Microsoft Office and Microsoft Office Services and Web Apps;
- Microsoft Windows Codecs Library;
- Visual Studio;
- SQL Server;
- Microsoft Malware Protection Engine;
- .NET Core;
- .NET Repository;
- ASP .NET;
- Azure.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de enero, consta de 83 vulnerabilidades, 10 clasificadas como críticas y 73 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:

- Ejecución remota de código,
- Escalada de privilegios,
- Denegación de servicio,
- Divulgación de información,
- Elusión de medidas de seguridad,
- Suplantación de identidad (spoofing),
- Manipulación (tampering).

Etiquetas: Actualización, Microsoft, Navegador, Vulnerabilidad, Windows

---

Denegación de servicio en Junos OS y Junos OS Evolved

Fecha de publicación: 14/01/2021

Importancia: Crítica

Recursos afectados:

Junos OS:

- Todas las versiones anteriores a 17.3R3-S10, con la excepción de 15.1X49-D240 en la serie SRX y 15.1R7-S8 en la serie EX;
- 17.4, versiones anteriores a 17.4R2-S12, 17.4R3-S4;
- 18.1, versiones anteriores a 18.1R3-S12;
- 18.2, versiones anteriores a 18.2R2-S8, 18.2R3-S6;
- 18.3, versiones anteriores a 18.3R3-S4;
- 18.4, versiones anteriores a 18.4R1-S8, 18.4R2-S6, 18.4R3-S6;
- 19.1, versiones anteriores a 19.1R1-S6, 19.1R2-S2, 19.1R3-S3;

- 19.2, versiones anteriores a 19.2R3-S1;
- 19.3, versiones anteriores a 19.3R2-S5, 19.3R3-S1;
- 19.4, versiones anteriores a 19.4R1-S3, 19.4R2-S3, 19.4R3;
- 20.1, versiones anteriores a 20.1R2;
- 20.2, versiones anteriores a 20.2R1-S3 20.2R2;
- Versiones 20.3 anteriores a 20.3R1-S1, 20.3R2.

Junos OS Evolved las siguientes versiones:

- Todas las versiones anteriores a 20.3R1-S1-EVO, 20.3R2-EVO.

Descripción:

Juniper ha informado de una vulnerabilidad que podría provocar una denegación en los servicios de Juniper Networks Junos OS y Junos OS Evolved Routing Protocol Daemon (RPD) al recibir un mensaje específico de BGP FlowSpec.

Solución:

Las siguientes versiones solucionan esta vulnerabilidad:

- Junos OS: 15.1R7-S8, 15.1X49-D240, 17.3R3-S10, 17.4R2-S12, 17.4R3-S4, 18.1R3-S12, 18.2R2-S8, 18.2R3-S6, 18.3R3-S4, 18.4R1-S8, 18.4R2-S6, 18.4R3-S6, 19.1R2-S2, 19.1R3-S3, 19.2R3-S1, 19.3R2-S5, 19.3R3-S1, 19.4R1-S3, 19.4R2-S3, 19.4R3, 20.1R2, 20.2R1-S3, 20.2R2, 20.3R1-S1, 20.3R2, 20.4R1, y todas las versiones posteriores.
- Junos OS Evolved: 20.3R1-S1-EVO, 20.3R2-EVO, 20.4R1-EVO y todas las versiones posteriores.

Se requiere la siguiente configuración mínima para solucionar potencialmente este problema: *protocols bgp family inet flow*

Detalle:

La vulnerabilidad de verificación inadecuada, encontrada en los servicios de Juniper Networks Junos OS y Junos OS Evolved Routing Protocol Daemon (RPD), permite que un atacante envíe un mensaje BGP FlowSpec válido, causando un cambio inesperado en los anuncios de ruta dentro del dominio BGP FlowSpec. El envío sostenido de estos mensajes provoca interrupciones en el tráfico de la red y causan una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2021-0211 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 14/01/2021

Importancia: Crítica

Recursos afectados:

- Jenkins weekly, versiones 2.274 y anteriores;
- Jenkins LTS, versiones 2.263.1 y anteriores.

Descripción:

Se han publicado varias vulnerabilidades en el core de Jenkins, 6 de severidad alta, 3 medias y una baja.

Solución:

- Jenkins weekly, actualizar a la versión 2.275;
- Jenkins LTS, actualizar a la versión 2.263.2.

Detalle:

Los tipos de vulnerabilidades publicadas, de severidad alta, se corresponden con los siguientes:

- 2 vulnerabilidades de Cross-Site Scripting (*XSS*). Se han asignado los identificadores CVE-2021-21603 y CVE-2021-21608 para estas vulnerabilidades.
- 1 vulnerabilidad de Cross-Site Scripting (*XSS*) reflejado. Se ha asignado el identificador CVE-2021-21610 para esta vulnerabilidad.
- 1 vulnerabilidad de Cross-Site Scripting (*XSS*) almacenado. Se ha asignado el identificador CVE-2021-21611 para esta vulnerabilidad.
- 1 vulnerabilidad de deserialización de datos no confiables. Se ha asignado el identificador CVE-2021-21604 para esta vulnerabilidad.
- 1 vulnerabilidad de validación incorrecta de los datos de entrada. Se ha asignado el identificador CVE-2021-21605 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han asignado los identificadores CVE-2021-21602, CVE-2021-21606, CVE-2021-21607 y CVE-2021-21609.

Etiquetas: Actualización, Vulnerabilidad

Deserialización XML insegura en productos de Red Hat

Fecha de publicación: 14/01/2021

Importancia: Crítica

Recursos afectados:

- Decision Manager, versión 7.9.1;
- Process Automation Manager, versión 7.9.1.

Descripción:

Red Hat ha publicado una vulnerabilidad de severidad crítica de tipo deserialización XML insegura.

Solución:

Actualizar:

- Process Automation Manager a la versión 7.9.1.
- Decision Manager a la versión 7.9.1.

Detalle:

Un atacante podría ejecutar código de forma remota debido a una deserialización XML insegura en listas de bloques. Se ha asignado el identificador CVE-2020-26217 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Múltiples vulnerabilidades en AirWave Glass de Aruba

Fecha de publicación: 14/01/2021

Importancia: Crítica

Recursos afectados:

AirWave Glass, versiones 1.3.2 y anteriores.

Descripción:

Aruba ha publicado 3 vulnerabilidades de severidad crítica y otra de severidad alta, que podrían permitir el acceso a la interfaz de administración web o el compromiso total del sistema operativo del host subyacente al entorno Airwave Glass.

Solución:

Actualizar a la versión 1.3.3 o posterior.

Detalle:

- Las peticiones manipuladas del lado del servidor (Server-Side Request Forgery (*SSRF*)) a través de un endpoint final, no autenticado, podrían permitir a un atacante la divulgación de información sensible para omitir la autenticación y obtener acceso de administrador en la interfaz de administración web. Se ha asignado el identificador CVE-2020-24641 para esta vulnerabilidad.
- Un atacante podría ejecutar comandos arbitrarios en un entorno de contenedores dentro de Airwave Glass y comprometer el sistema operativo del host subyacente, mediante una validación insuficiente de los datos de entrada o una deserialización insegura de Java. Se han asignado los identificadores CVE-2020-24640 y CVE-2020-24639 para estas vulnerabilidades.
- Múltiples vulnerabilidades de ejecución remota de código en Airwave Glass, a través de la *cli. Glassadmin*, podrían permitir a un atacante con privilegios de *glassadmin* ejecutar código arbitrario, como root, en el sistema operativo host subyacente. Se ha asignado el identificador CVE-2020-24638 para la vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en Dnsmasq

Fecha de publicación: 20/01/2021

Importancia: Alta

Recursos afectados:

Dnsmasq DNS y servidor DHCP, versión 2.8.2 y anteriores.

Descripción:

Múltiples vulnerabilidades en la implementación de la DNSSEC dnsmasq podrían permitir a un atacante remoto, no autenticado, envenenar la caché, divulgar información, ejecutar código arbitrario o causar una condición de denegación de servicio (DoS) en un dispositivo afectado. Las vulnerabilidades se agrupan y se denominan DNSpooq.

Solución:

- Actualizar a dnsmasq 2.83.
- Los usuarios de sistemas IoT o embebidos, deberán consultar con su fabricante.
- Se recomienda hacer uso de las buenas prácticas de seguridad siguientes para proteger la infraestructura DNS:
    - Proteja a sus clientes de DNS utilizando *stateful-inspection firewalls* que proporcionen seguridad al DNS (por ejemplo, los *stateful-inspection firewalls* y los dispositivos NAT pueden bloquear las respuestas no solicitadas del DNS, la inspección de la capa de aplicación del DNS puede evitar el reenvío de paquetes de DNS anómalos).
    - Proporcionar un servicio seguro de recursividad del DNS con características como la validación DNSSEC y la codificación 0x20 bits como parte de los servicios de DNS, cuando corresponda.
    - Prevenir la exposición de dispositivos de IoT y otros dispositivos directamente a través de Internet, para minimizar el abuso del DNS.
    - Implementar una configuración Secure By Default adecuada a su entorno.

Detalle:

- Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*Heap*) debida a la ordenación de los RRSets antes de validarlos con los datos de DNSSEC, podría permitir a un atacante ejecutar código arbitrario mediante el envío de una respuesta DNS especialmente diseñada. Se ha asignado el identificador CVE-2020-25681 para esta vulnerabilidad.
- Una vulnerabilidad de desbordamiento de búfer basado en memoria dinámica (*Heap*) debida a la extracción de nombres de paquetes DNS antes de validarlos con los datos de DNSSEC, podría permitir a un atacante ejecutar código arbitrario mediante el envío de una respuesta DNS especialmente diseñada. Se ha asignado el identificador CVE-2020-25682 para esta vulnerabilidad.
- Las vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (*Heap*) cuando DNSSEC está activado, antes de validar las entradas recibidas, podría permitir a un atacante denegar el servicio mediante el envío de respuestas DNS válidas. Se ha asignado el identificador CVE-2020-25683 y CVE-2020-25687 para estas vulnerabilidades.
- La validación insuficiente de la autenticidad de los datos en la respuesta de una consulta reenviada cuando Dnsmasq comprueba en forward.c:reply_query() si la dirección / puerto de destino de la respuesta, es utilizada por las consultas reenviadas pendientes, podría permitir a un atacante realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25684 para esta vulnerabilidad.
- El uso de un algoritmo criptográfico roto o débil podría permitir a un atacante encontrar varios dominios diferentes con el mismo hash fuera de ruta, reduciendo considerablemente el número de intentos de falsificar una respuesta para su aceptación por parte de Dnsmasq, y realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25685 para esta vulnerabilidad.
- La validación insuficiente de la autenticidad de los datos, al recibir una consulta en la que Dnsmasq no comprueba si existe una solicitud pendiente con el mismo nombre antes de reenviar una nueva solicitud, podría permitir a un atacante, fuera de la ruta de la red, reducir considerablemente el número de intentos de falsificar una respuesta para su aceptación por parte de Dnsmasq, y realizar un ataque de envenenamiento de la caché del DNS. Se ha asignado el identificador CVE-2020-25686 para esta vulnerabilidad.

Etiquetas: Actualización, Comunicaciones, DNS, Vulnerabilidad

---

Actualizaciones críticas en Oracle (enero 2021)

Fecha de publicación: 20/01/2021

Importancia: Crítica

Recursos afectados:

- Business Intelligence Enterprise Edition, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Enterprise Manager Base Platform, versiones 13.2.1.0, 13.3.0.0 y 13.4.0.0;
- Enterprise Manager for Fusion Applications, versión 13.3.0.0;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- Hyperion Financial Reporting, versión 11.1.2.4;
- Hyperion Infrastructure Technology, versión 11.1.2.4;
- Instantis EnterpriseTrack, versiones de la 17.1 a la 17.3;
- JD Edwards EnterpriseOne Orchestrator, todas las versiones anteriores a la 9.2.5.1;
- JD Edwards EnterpriseOne Tools, todas las versiones anteriores a la 9.2.5.0;
- MySQL Client, versiones 5.6.50 y anteriores, 5.7.32 y anteriores, 8.0.22 y anteriores;
- MySQL Enterprise Monitor, versiones 8.0.22 y anteriores;
- MySQL Server, versiones 5.6.50 y anteriores, 5.7.32 y anteriores, 8.0.22 y anteriores;
- MySQL Workbench, versiones 8.0.22 y anteriores;
- Oracle Adaptive Access Manager, versión 11.1.2.3.0;
- Oracle Agile Engineering Data Management, versión 6.2.1.0;
- Oracle Agile PLM, versiones 9.3.5 y 9.3.6;
- Oracle Agile Product Lifecycle Management for Process, versión 6.1;
- Oracle Application Express Opportunity Tracker, todas las versiones anteriores a la 20.2;
- Oracle Application Express Survey Builder, todas las versiones anteriores a la 20.2;
- Oracle Application Testing Suite, versión 13.3.0.1;
- Oracle Argus Safety, versión 8.2.2;
- Oracle BAM (Business Activity Monitoring), versiones 11.1.1.9.0 y 12.2.1.3.0;
- Oracle Banking Corporate Lending Process Management, versiones 14.1.0, 14.3.0 y 14.4.0;
- Oracle Banking Credit Facilities Process Management, versiones 14.1.0, 14.3.0 y 14.4.0;
- Oracle Banking Extensibility Workbench, versiones 14.3.0 y 14.4.0;
- Oracle Banking Liquidity Management, versiones de la 14.0.0 a la 14.4.0;
- Oracle Banking Payments, versión 14.4.0;
- Oracle Banking Platform, versiones 2.4.0, 2.4.1, 2.6.2, 2.7.0, 2.7.1, 2.8.0 y 2.9.0;
- Oracle Banking Supply Chain Finance, versiones de la 14.2.0 a la 14.4.0;
- Oracle Banking Trade Finance Process Management, versiones 14.1.0, 14.3.0 y 14.4.0;
- Oracle Banking Virtual Account Management, versiones 14.1.0, 14.3.0 y 14.4.0;
- Oracle BI Publisher, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;

- Oracle Business Process Management Suite, versiones 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Coherence, versiones 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0;
- Oracle Communications Application Session Controller, versión 3.9m0p2;
- Oracle Communications ASAP, versión 7.3;
- Oracle Communications BRM - Elastic Charging Engine, versiones 11.3.0.9 y 12.0.0.3;
- Oracle Communications Calendar Server, versión 8.0.0.4.0;
- Oracle Communications Contacts Server, versión 8.0.0.5.0;
- Oracle Communications Diameter Signaling Router (DSR), versiones de la 8.0.0 a la 8.2.2;
- Oracle Communications Element Manager, versiones de la 8.2.1.0 a la 8.2.2.1;
- Oracle Communications MetaSolv Solution, versiones de la 6.3.0 a la 6.3.1;
- Oracle Communications Network Charging and Control, versiones 6.0.1 y 12.0.2;
- Oracle Communications Operations Monitor, versiones 3.4, 4.1, 4.2 y 4.3;
- Oracle Communications Performance Intelligence Center (PIC) Software, versión 10.4.0.2;
- Oracle Communications Session Report Manager, versiones de la 8.2.1.0 a la 8.2.2.1;
- Oracle Complex Maintenance, Repair, and Overhaul, versiones 11.5.10, 12.1 y 12.2;
- Oracle Configurator, versiones 12.1 y 12.2;
- Oracle Data Integrator, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Database Server, versiones 12.1.0.2, 12.2.0.1, 18c y 19c;
- Oracle E-Business Suite, versiones de la 12.1.1 a la 12.1.3 y de la 12.2.3 a la 12.2.10;
- Oracle Endeca Information Discovery Integrator, versión 3.2.0.0;
- Oracle Enterprise Communications Broker, versiones 3.1 y 3.2;
- Oracle Enterprise Data Quality, versiones 11.1.1.9.0 y 12.2.1.3.0;
- Oracle Enterprise Repository, versión 11.1.1.7.0;
- Oracle Financial Services Analytical Applications Infrastructure, versiones de la 8.0.6 a la 8.1.0;
- Oracle Financial Services Asset Liability Management, versiones 8.0.7 y 8.1.0;
- Oracle Financial Services Data Integration Hub, versiones 8.0.3 y 8.0.6;
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.6, 8.0.7 y 8.1.0;
- Oracle Financial Services Market Risk Measurement and Management, versión 8.0.6;
- Oracle Financial Services Profitability Management, versiones 8.0.6, 8.0.7 y 8.1.0;
- Oracle Financial Services Revenue Management and Billing, versiones 2.9.0.0 y 2.9.0.1;
- Oracle FLEXCUBE Core Banking, versiones de la 11.5.0 a la 11.9.0 ;
- Oracle FLEXCUBE Universal Banking, versión 14.4.0;
- Oracle Fusion Middleware MapViewer, versión 12.2.1.3.0;
- Oracle Global Lifecycle Management OPatch;
- Oracle Global Lifecycle Manager;
- Oracle GoldenGate Application Adapters, versión 19.1.0.0.0;
- Oracle GraalVM Enterprise Edition, versiones 19.3.4 y 20.3.0;
- Oracle Health Sciences Information Manager, versión 3.0.1;
- Oracle Healthcare Master Person Index, versión 4.0.2.5;
- Oracle Hospitality Reporting and Analytics, versión 9.1.0 ;
- Oracle Hospitality Simphony, versiones 18.2.7.2 y 19.1.3;
- Oracle Insurance Allocation Manager for Enterprise Profitability, versión 8.1.0;
- Oracle Insurance Insbridge Rating and Underwriting, versiones 5.0.0.20 y 5.1.1.3;
- Oracle Insurance Policy Administration, versiones 10.2.0, 10.2.4, 11.0.2 y de la 11.1.0 a la 11.3.0;
- Oracle Insurance Rules Palette, versiones 10.2.0, 10.2.4, 11.0.2 y de la 11.1.0 a la 11.3.0;
- Oracle Java SE, versiones 7u281 y 8u271;
- Oracle Java SE Embedded, versión 8u271;
- Oracle Managed File Transfer, versiones 12.2.1.3.0 y 12.2.1.4.0;
- Oracle Outside In Technology, versiones 8.5.4 y 8.5.5;
- Oracle Real-Time Decision Server, versión 3.2.1.0;
- Oracle Retail Assortment Planning, versión 16.0.3;
- Oracle Retail Bulk Data Integration, versiones 15.0.3 y 16.0.3;
- Oracle Retail Customer Management and Segmentation Foundation, versiones 16.0, 17.0, 18.0 y 19.0;
- Oracle Retail Extract Transform and Load, versiones 13.2.5 y 13.2.8;
- Oracle Retail Financial Integration, versiones 14.1.3, 15.0.3 y 16.0.3;
- Oracle Retail Integration Bus, versiones 14.1.3, 15.0.3 y 16.0.3;
- Oracle Retail Invoice Matching, versiones 13.2, 14.0 y 14.1;
- Oracle Retail Merchandising System, versión 15.0;
- Oracle Retail Order Broker, versiones 15.0 y 16.0;
- Oracle Retail Order Broker Cloud Service, versión 15.0;
- Oracle Retail Sales Audit, versión 14.1;
- Oracle Retail Service Backbone, versiones 14.1.3, 15.0.3 y 16.0.3;
- Oracle Retail Store Inventory Management, versiones 14.0.4.0, 14.1.3.0, 14.1.3.9, 15.0.3.0 y 16.0.3.0;
- Oracle SD-WAN Edge, versión 9.0;
- Oracle Secure Backup;
- Oracle Transportation Management, versión 1.4.3;
- Oracle Utilities Framework, versiones 4.2.0.2.0, 4.2.0.3.0, de la 4.3.0.1.0 a la 4.3.0.6.0, 4.4.0.0.0 y 4.4.0.2.0;
- Oracle VM VirtualBox, todas las versiones anteriores a la 6.1.18;
- Oracle WebCenter Portal, versiones 11.1.1.9.0, 12.2.1.3.0 y 12.2.1.4.0;
- Oracle WebCenter Sites, versiones 12.2.1.3.0 y 12.2.1.4.0;
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0;
- Oracle ZFS Storage Appliance Kit, versión 8.8;
- PeopleSoft Enterprise FIN Payables, versión 9.2;
- PeopleSoft Enterprise HCM Human Resources, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.56, 8.57 y 8.58;
- Primavera Gateway, versiones de la 16.2.0 a la 16.2.11, de la 17.12.0 a la 17.12.9, de la 18.8.0 a la 18.8.10 y de la 19.12.0 a la 19.12.10;
- Primavera P6 Enterprise Project Portfolio Management, versiones de la 16.1.0 a la 16.2.20, de la 17.1.0 a la 17.12.19, de la 18.1.0 a la 18.8.21 y de la 19.12.0 a la 19.12.10;
- Primavera Unifier, versiones 16.1, 16.2, de la 17.7 a la 17.12, 18.8, 19.12 y 20.12;
- Siebel Applications, versiones 20.12 y anteriores;
- StorageTek Tape Analytics SW Tool, versión 2.3.1;

Descripción:

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

Solución:

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

Detalle:

Esta actualización resuelve un total de 329 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, Vulnerabilidad

Vulnerabilidad en el core de Drupal

Fecha de publicación: 21/01/2021

Importancia: Crítica

Recursos afectados:

Versiones anteriores a:

- 9.1.3;
- 9.0.11;
- 8.9.13;
- 7.78.

Descripción:

Se han publicado una vulnerabilidad de severidad crítica, en la librería Archive_Tar, que afecta al core de Drupal.

Solución:

Actualizar a las versiones 9.1.3, 9.0.11, 8.9.13, 7.78.

Las versiones de Drupal 8, anteriores a la 8.9.x, están al final de su vida útil y ya no reciben cobertura de seguridad.

Detalle:

La comprobación inadecuada de los enlaces simbólicos en la librería Archive_Tar podría permitir operaciones de escritura con *Directory Traversal* . Se ha asignado el identificador CVE-2020-36193 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en productos de Cisco

Fecha de publicación: 21/01/2021

Importancia: Crítica

Recursos afectados:

- Cisco DNA Center Software, versiones 1.3.1.0 y anteriores;
- Cisco Smart Software Manager Satellite, versiones 5.1.0 y anteriores;
- los siguientes productos, si ejecutan una versión vulnerable de Cisco SD-WAN Software:
  - SD-WAN vBond Orchestrator Software;
  - SD-WAN vEdge Cloud Routers;
  - SD-WAN vEdge Routers;
  - SD-WAN vManage Software;
  - SD-WAN vSmart Controller Software;
  - IOS XE SD-WAN Software.

Descripción:

Se han identificado 14 vulnerabilidades en productos de Cisco, de las que 6 son de severidad crítica y podrían permitir a un atacante remoto ejecutar comandos arbitrarios o provocar una condición de desbordamiento de búfer.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas se pueden descargar desde el panel de descarga de Software de Cisco. Para información más detallada, consulte la sección Referencias.

Detalle:

Un atacante remoto y no autenticado podría ejecutar comandos arbitrarios aprovechando una validación incorrecta de entrada en la interfaz de usuario web de SD-WAN vManage Software, en la herramienta Command Runner de DNA Center o en la interfaz de usuario web Smart Software Manager Satellite, enviando una entrada especialmente diseñada. Se han asignado los identificadores CVE-2021-1299, CVE-2021-1264, CVE-2021-1138, CVE-2021-1140 y CVE-2021-1142 para estas vulnerabilidades, respectivamente.

Una vulnerabilidad de manejo incorrecto del tráfico IP podría permitir a un atacante enviar tráfico IP, especialmente diseñado, y provocar un desbordamiento de búfer. Se ha asignado el identificador CVE-2021-1300 para esta vulnerabilidad.

Para las vulnerabilidades de severidad alta se han asignado los identificadores CVE-2021-1261, CVE-2021-1260, CVE-2021-1139 y CVE-2021-1141.
Para las vulnerabilidades de severidad media se han asignado los identificadores CVE-2021-1263, CVE-2021-1262, CVE-2021-1298 y CVE-2021-1301.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Moodle

Fecha de publicación: 25/01/2021

Importancia: Crítica

Recursos afectados:

- Versión 3.10;
- desde la versión 3.9, hasta la 3.9.3;
- desde la versión 3.8, hasta la 3.8.6;
- desde la versión 3.5, hasta la 3.5.15;
- versiones anteriores sin soporte.

Descripción:

Se han publicado 5 vulnerabilidades en Moodle, 3 de severidad crítica y 2 de severidad baja, que podrían permitir ataques de tipo XSS, la ejecución arbitraria de código PHP, la divulgación de información o la denegación de servicio en el lado del cliente.

Solución:

Aplicar las siguientes actualizaciones, en función de la versión afectada:

- 3.10.1;
- 3.9.4;
- 3.8.7;
- 3.5.16.

Detalle:

- La validación insuficiente de las consultas de búsqueda, desde la plantilla de búsqueda de entradas, podría permitir a un atacante llevar a cabo ataques XSS reflejados. Se ha asignado el identificador CVE-2021-20183 para esta vulnerabilidad.
- El saneado insuficiente del contenido TeX, cuando el filtro de notación TeX está activado, podría permitir a un atacante llevar a cabo ataques del tipo XSS almacenado. Se ha asignado el identificador CVE-2021-20186 para esta vulnerabilidad.
- Los administradores del sitio podrían ejecutar *scripts* PHP arbitrarios a través de un *include* PHP, utilizado durante la autenticación de Shibboleth. Se ha asignado el identificador CVE-2021-20187 para esta vulnerabilidad.

Para el resto de vulnerabilidades, de severidad baja, se han asignado los identificadores CVE-2021-20184 y CVE-2021-20185.

Etiquetas: Actualización, CMS, Vulnerabilidad

Vulnerabilidad 0-day en SMA 100 de SonicWall

Fecha de publicación: 25/01/2021

Importancia: Alta

Recursos afectados:

Los productos que se encuentran bajo investigación corresponden a SMA 100 Series (SMA 200, SMA 210, SMA 400, SMA 410 y SMA 500v Virtual appliance).

Descripción:

SonicWall continúa investigando una posible vulnerabilidad, de severidad alta, de tipo 0-day.

Solución:

Se pide a los administradores de la serie SMA 100, mientras dure la investigación:

- Utilizar un *firewall* con reglas que permitan sólo conexiones SSL-VPN a la aplicación SMA desde direcciones IP conocidas o incluidas en una lista blanca. Para ello, consultar el siguiente enlace.
- Crear reglas de acceso específicas o deshabilitar el acceso administrativo mediante HTTPS y Virtual Office, desde Internet, mientas dure la investigación.

Detalle:

SonicWall identificó un ataque coordinado contra sus sistemas internos por parte de actores de amenazas muy sofisticadas, que explotaban probables vulnerabilidades 0-day en ciertos productos de acceso remoto seguro de SonicWall.

Etiquetas: 0day, Comunicaciones, Vulnerabilidad

Vulnerabilidad de denegación de servicio en Xen

Fecha de publicación: 27/01/2021

Importancia: Alta

Recursos afectados:

Xen, versiones 4.12.3, 4.12.4 y todas las versiones 4.13.1 y siguientes.

Descripción:

Xen ha informado de una vulnerabilidad en sistemas x86 en la que un invitado HVM con dispositivos *PCI pass through* puede agotar los recursos PCI disponibles de otros invitados o de todo el host, provocando una denegación de servicio.

Solución:

Xen ha publicado un parche para las versiones 4.14 - 4.12 y para la versión unstable.

Detalle:

La vulnerabilidad detectada solo afecta a los sistemas x86 que ejecutan invitados HVM con dispositivos *PCI pass through*. Un atacante podría forzar la asignación de todos los vectores IDT en el sistema, causando el agotamiento de los recursos PCI y causando así la denegación del servicio. Se ha asignado el identificador CVE-2021-3308 para esta vulnerabilidad.

Etiquetas: Actualización, Virtualización, Vulnerabilidad

Vulnerabilidad de desbordamiento de búfer en sudo

Fecha de publicación: 27/01/2021

Importancia: Crítica

Recursos afectados:

Sudo, versiones:

- desde la 1.8.2, hasta la 1.8.31p2;
- desde la 1.9.0, hasta la 1.9.5p1.

Descripción:

Qualys Research Team ha reportado a *sudo* una vulnerabilidad, de tipo desbordamiento de búfer basado en memoria dinámica (*heap*), que podría permitir la escalada de privilegios.

Solución:

Actualizar a la versión 1.9.5p2 de *sudo*.

Detalle:

La vulnerabilidad, denominada *Baron Samedit* por sus descubridores, podría ser aprovechada por cualquier usuario local, no autenticado, para escalar privilegios a nivel de *root*, incluso si el usuario no aparece en el archivo *sudoers*. El fallo se encuentra en el código que escapa los caracteres especiales en los argumentos de los comandos cuando *sudo* ejecuta un comando en modo *shell*. Se ha asignado el identificador CVE-2021-3156 para esta vulnerabilidad.

Etiquetas: Actualización, Linux, Vulnerabilidad

Múltiples vulnerabilidades 0day en productos de Apple

Fecha de publicación: 27/01/2021

Importancia: Crítica

Recursos afectados:

- iOS, versiones anteriores a 14.4;
- iPadOS, versiones anteriores a 14.4.

Descripción:

Un investigador anónimo ha informado a Apple de tres vulnerabilidades, de tipo 0day, que podrían permitir a un atacante realizar una escalada de privilegios o ejecutar código arbitrario de forma remota.

Solución:

Actualizar a las versiones iOS 14.4 y iPadOS 14.4, siguiendo los pasos indicados en la web y que están disponibles para los siguientes productos:

- iPhone 6s y posteriores,
- iPad Air 2 y posteriores, iPad mini 4 y posteriores,
- iPod touch (séptima generación).

Detalle:

- Una aplicación malintencionada podría permitir a un atacante realizar una escalada de privilegios aprovechando una vulnerabilidad de condición de carrera que afecta al Kernel. Se ha asignado el identificador CVE-2021-1782 para esta vulnerabilidad.
- Un atacante remoto podría ejecutar código arbitrario aprovechando vulnerabilidades de lógica que afectan a WebKit. Se han asignado los identificadores CVE-2021-1871 y CVE-2021-1870 para estas vulnerabilidades.

Apple ha informado de que estas vulnerabilidades pueden haber sido explotadas activamente.

Etiquetas: 0day, Actualización, Apple, Vulnerabilidad