Boletín de Junio de 2018

Avisos Técnicos

Escalado de privilegios en InfoSphere Information Server de IBM

Fecha de publicación: 04/06/2018

Importancia: Alta

Recursos afectados:

- IBM Information Server Framework: versiones 9.1, 11.3, 11.5 y 11.7
- IBM InfoSphere Information Server Cloud versiones 11.5 y 11.7

Descripción:

IBM ha detectado una vulnerabilidad de criticidad alta que podría permitir a un atacante escalar privilegios.

Solución:

IBM recomienda actualizar los productos afectados a la última versión disponible:

- IBM InfoSphere Information Server versión 11.7.0.1
- IBM InfoSphere Information Server versión 11.5.0.2
- IBM InfoSphere Information Server Framework parche de seguridad

Detalle:

IBM InfoSphere Information Server podría permitir que un usuario realice un escalado de privilegios pudiendo conseguir permisos de administrador debido a que los controles de acceso son incorrectos. Se ha reservado el identificador CVE-2017-1350 para esta vulnerabilidad

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 07/06/2018

Importancia: Crítica

Recursos afectados:

- Cisco Prime Collaboration Provisioning (PCP) versiones 12.2 y anteriores
- Cisco AsyncOS versiones de software WSA 10.5.1, 10.5.2 y 11.0.0
- Cisco Network Services Orchestrator (NSO) versiones 4.1 hasta la 4.1.6.0; 4.2 hasta la 4.2.4.0; 4.3 hasta la 4.3.3.0 y 4.4 hasta la 4.4.2.0
- Cisco IP Phone 6800, 7800 y 8800 con una versión de firmware multiplataforma anterior a la 11.1(2)
- Los productos Prime Collaboration Assurance y Prime Collaboration Provisioning.
- Los siguientes productos basados en Cisco Voice Operating System (VOS):
  - Emergency Responder.
  - Finesse.
  - Hosted Collaboration Mediation Fulfillment.
  - MediaSense.
  - Prime License Manager.
  - SocialMiner.
  - Unified Communications Manager (UCM).
  - Unified Communications Manager IM and Presence Service (IM&P) (las versiones anteriores eran conocidas como Cisco Unified Presence).

    - Unified Communication Manager Session Management Edition (SME).
    - Unified Contact Center Express (UCCx).
    - Unified Intelligence Center (UIC).
    - Unity Connection y Virtualized Voice Browser.
- Cisco Meeting Server (CMS) 2000 Platforms ejecutando versiones de Software CMS anterior a la 2.2.13 o la versión 2.3.4
- Cisco ASA Software y Cisco Firepower Threat Defense (FTD) Software, sobre los siguientes productos:
    - 3000 Series Industrial Security Appliance (ISA).
    - ASA 1000V Cloud Firewall.
    - ASA 5500 Series Adaptive Security Appliances.
    - ASA 5500-X Series Next-Generation Firewalls.
    - ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers.
    - Adaptive Security Virtual Appliance (ASAv).
    - Firepower 2100 Series Security Appliance.
    - Firepower 4100 Series Security Appliance.
    - Firepower 9300 ASA Security Module.
    - FTD Virtual (FTDv).
- Cisco Unified IP Phone software.
- Cisco WebEx.
- Cisco Wide Area Application Services (WAAS) Software con la configuración por defecto.
- Cisco Integrated Management Controller Supervisor Software y Cisco UCS Director Software.
- Cisco Unified Computing System (UCS) Software.
- Cisco Prime Collaboration Provisioning.
- Cisco Identity Services Engine (ISE).
- Cisco Unified Communications Manager.
- Cisco Unity Connection.
- Cisco FireSIGHT System Software.
- Cisco AnyConnect Network Access Manager y Cisco AnyConnect Secure Mobility Client for iOS, Mac OS X, Android, Windows y Linux

Descripción:

Cisco ha publicado 28 vulnerabilidades en diversos productos, siendo 2 vulnerabilidades de severidad crítica, 11 de severidad alta y 15 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 un puerto abierto en el servicio Network Interface and Configuration Engine (NICE) que un atacante podría explotar, accediendo al sistema RMI abierto en una instancia de PCP afectada. Se podrían realizar acciones maliciosas que afecten al PCP y a los dispositivos conectados a él.Se ha reservado el identificador CVE-2018-0321 para esta vulnerabilidad.

- Una vulnerabilidad debida a operaciones de memoria incorrectas cuando el software afectado analiza un nombre de usuario durante la autenticación de inicio de sesión que podría permitir a un atacante ejecutar código arbitrario en el dispositivo o causar su sobrerecarga, resultando en una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2018-0315 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los siguientes identificadores: CVE-2018-0353, CVE-2018-0320, CVE-2018-0318, CVE-2018-0319, CVE-2018-0317, CVE-2018-0322, CVE-2018-0274, CVE-2018-0316, CVE-2017-6779, CVE-2018-0263, CVE-2018-0296, CVE-2018-0332, CVE-2018-0357, CVE-2018-0356, CVE-2018-0329, CVE-2018-0352, CVE-2018-0149, CVE-2018-0338, CVE-2018-0340, CVE-2018-0336, CVE-2018-0339, CVE-2018-0355, CVE-2018-0354, CVE-2018-0335, CVE-2018-0333, CVE-2018-0334.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Security Identity Manager de IBM

Fecha de publicación: 08/06/2018

Importancia: Alta

Recursos afectados:

- IBM Security Identity Manager versiones 7.0 y 7.0.1.

Descripción:

IBM ha detectado 5 vulnerabilidades: una de ellas es de criticidad alta, 2 son de criticidad media y las 2 restantes de criticidad baja.

Solución:

Según la versión del producto afectado hay que aplicar distintas mitigaciones:

- Versión7.0: Contactar con el servicio de soporte de IBM.
- Versión 7.0.1: Descargar la actualización 7.0.1-ISS-SIM-FP0009.

Detalle:

La vulnerabilidad de criticidad alta podría permitir a un atacante autenticado subir archivos maliciosos que podrían ser procesados automÃiticamente en el entorno. Se ha reservado el identificador CVE-2018-1453 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Vulnerabilidades en productos Asterisk

Fecha de publicación: 12/06/2018

Importancia: Crítica

Recursos afectados:

- Asterisk Open Source:
  - 13.x desde la versión 13.10.0 y anteriores.
  - 14.x todas las versiones.
  - 15.x todas las versiones.
- Certified Asterisk 13.18 y 13.21 todas las versiones.

Descripción:

Asterisk ha publicado dos boletines de seguridad, uno de ellos de severidad crítica y otro baja, que podrían permitir a un atacante causar una denegación de servicio o acceder a información confidencial.

Solución:

Asterisk recomienda actualizar los productos afectados:

- Asterisk Open Source actualizar a las versiones 15.4.1, 13.21.1 y 14.7.7.
- Certified Asterisk actualizar a las versiones 13.18-cert4 y 13.21-cert2.

Detalle:

Cuando se hace una conexión a Asterisk vía TCP/TLS y el cliente se desconecta de forma repentina o envía un mensaje especialmente diseñado, puede provocar que el servicio entre en bucle infinito pudiendo causar una denegación de servicio.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en AirWatch Agent de VMware

Fecha de publicación: 12/06/2018

Importancia: Crítica

Recursos afectados:

- VMware AirWatch Agent para Android (A/W Agent)
- VMware AirWatch Agent para Windows Mobile (A/W Agent)

Descripción:

Se ha detectado una vulnerabilidad crítica que podría permitir a un atacante remoto realizar ejecución de código, creación y ejecución no autorizada de archivos y acceso a directorios públicos.

Solución:

Desde VMware han publicado actualizaciones dependiendo del dispositivo afectado:

- Para dispositivos Android, actualizar la aplicación a la versión AirWatch Agent 8.2 disponible en Google Play.
- Para dispositivos Windows Mobile, actualizar la aplicación a la versión Agent 6.5.2 disponible desde este enlace.

Detalle:

La vulnerabilidad podría permitir a un atacante remoto la ejecución de código y la posibilidad de emplear el gestor de archivos en tiempo real, así como la creación y ejecución no autorizada de archivos en Agent sandbox, permitiendo también el acceso por parte de un administrador malintencionado a directorios públicos como, por ejemplo, los de la tarjeta SD. Se ha reservado el identificador CVE-2018-6968 para esta vulnerabilidad.

Etiquetas: Actualización, VMware, Vulnerabilidad

Boletín de seguridad de Microsoft de junio de 2018

Fecha de publicación: 13/06/2018

Importancia: Crítica

Recursos afectados:

- Internet Explorer.
- Microsoft Edge.
- Microsoft Windows.
- Microsoft Office y Microsoft Office Services y Web Apps.
- ChakraCore.
- Adobe Flash Player.

Descripción:

La publicación mensual de actualizaciones de seguridad de Microsoft de este mes consta de 50 vulnerabilidades, 10 clasificadas como críticas y 40 como importantes, siendo el resto de las vulnerabilidades publicadas en el boletín de severidad media o baja.

Solución:

Instalar la actualización correspondiente. En la pÃigina 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 junio 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.

Etiquetas: Actualización, Microsoft, Navegador, Sistema Operativo, Vulnerabilidad

---

Actualización de seguridad de SAP de junio 2018

Fecha de publicación: 14/06/2018

Importancia: Crítica

Recursos afectados:

- SAP Business One, versiones 9.2 y 9.3
- SAP Internet Sales, versiones 7.30,7.31, 7.32, 7.33 y 7.54
- SAP Business Objects CMC, BI Launchpad, Friorified BI Launchpad, versiones 4.0, 4.10, 4.20 y 4.30
- SAP Business Objects Enterprise, versiones 4.0 y 4.1
- SAP UI5
- SAP UI5 Handler
- SAP Identity Management, version 8.0

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 10 notas de seguridad de las cuales, 3 son actualizaciones de notas de seguridad publicadas con anterioridad, siendo 2 de ellas de severidad crítica, 4 de de severidad alta y 4 de severidad media.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 2 vulnerabilidades de inyección de código
- 2 vulnerabilidad de divulgación de información
- 1 vulnerabilidad de denegación de servicio
- 1 vulnerabilidad de falta de Cross-Site Scripting
- 1 vulnerabilidad de incorrecta validación de XML
- 3 vulnerabilidades de otras tipologías

Las vulnerabilidades mÃis relevantes son las siguientes:

- Divulgación de información en SAP Business One que permitiría a un atacante obtener información adicional (datos del sistema, información de depuración, etc.) que le ayudaría a aprender sobre el sistema y a planificar otros ataques.
- Un atacante no autorizado podría ejecutar comandos de forma remota con el mismo nivel de privilegios que el servicio que lo ejecutó, pudiendo acceder a archivos y directorios arbitrarios ubicados en un sistema de archivos de un servidor SAP, como por ejemplo al código fuente de la aplicación, la configuración y los archivos críticos del sistema. Esto le permitiría obtener información técnica crítica y de negocio.
- Un atacante puede utilizar una vulnerabilidad de denegación de servico en SAP Internet Sales para terminar un proceso de un componente vulnerable, haciendo que nadie pueda utilizarlo. Esto afectaría a los procesos de negocio, disponibilidad del sistema y por lo tanto a la reputación del negocio.

Etiquetas: Actualización, SAP, Vulnerabilidad

Escalada de privilegios en plataforma IBM Netezza

Fecha de publicación: 15/06/2018

Importancia: Alta

Recursos afectados:

- IBM Netezza Platform Software versiones de la 7.0.4 a la 7.2.1.6

Impacto:

Un usuario malintencionado sin privilegios elevados podría ejecutar comandos como superusuario en los productos afectados.

Solución:

Actualizar a la siguiente versión publicada por el fabricante:

IBM Netezza Platform Software v7.2.1.6-P1

Detalle:

Un usuario local podría modificar un fichero editable globalmente, de tal manera que podría llegar a usarse para la ejecución de comandos como usuario *root*. Se ha reservado el identificador CVE-2018-1460 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Acceso remoto no autorizado en HPE NFVD

Fecha de publicación: 19/06/2018

Importancia: Alta

Recursos afectados:

HPE Network Function Virtualization Director (NFVD) versiones 4.2.1 anteriores al parche 3 gui.

Descripción:

HPE ha identificado una vulnerabilidad en HPE Network Function Virtualization Director (NFVD) que podría permitir el acceso remoto y no autorizado a información sensible.

Solución:

- Aplicar el parche gui 3 de NFVD 4.2.1

Detalle:

Se ha identificado una vulnerabilidad de tipo acceso remoto no autorizado que podría permitir el acceso remoto a información sensible. Se ha reservado el identificador CVE-2018-7071 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 21/06/2018

Importancia: Crítica

Recursos afectados:

- MDS 9000 Series Multilayer Switches
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Line Cards and Fabric Modules
- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- UCS 6100 Series Fabric Interconnects
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- Nexus 3600 Platform Switches
- Nexus 2000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 1000V Series Switches
- Nexus 1100 Series Cloud Services Platforms
- Nexus 4000 Series Switches
- Firepower 4100 Series Next-Generation Firewall
- MDS 9000 Series Multilayer Director Switches
- Nexus 9000 Series Switches in NX-OS mode
- Firepower 2100 Series
- Nexus 4000 Series Switch
- Cisco TelePresence Video Communication Server (VCS) Expressway
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Unified Communications Domain Manager
- Cisco NX-OS Software.
- Acano X-Series
- Cisco Meeting Server 1000
- Cisco Meeting Server 2000
- Cisco Firepower Management Center
- Cisco 5000 Series Enterprise Network Compute System
- Cisco UCS E-Series Servers
- Cisco Meeting Server
- Cisco AnyConnect Secure Mobility Client for Windows Desktop

Descripción:

Cisco ha publicado 33 vulnerabilidades en diversos productos, siendo 5 vulnerabilidades de severidad crítica, 19 de severidad alta y 9 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 debida a una incorrecta validación en los parÃimetros de entrada en el módulo de autenticación del subsistema NX-API, podría permitir a un atacante remoto sin autenticación enviar un paquete HTTP o HTTPS modificado a la interfaz de gestión del sistema afectado que tuviese la característica NX-API habilitada. Dicho paquete podría permitir la ejecución de código con permisos de root. Se ha reservado el identificador CVE-2018-0301 para esta vulnerabilidad.
- Una vulnerabilidad debida a una insuficiente validación de los valores en las cabeceras en los paquetes Cisco Fabric Services, podría permitir a un atacante remoto, sin autenticación, generar un paquete modificado y enviarlo a un dispositivo afectado, dicho paquete podría provocar un desbordamiento de búfer, conllevando a una ejecución de código arbitrario o a la denegación de servicio (DoS). Se ha reservado el identificador CVE-2018-0308 para esta vulnerabilidad.
- Una vulnerabilidad en el componente Cisco Fabric Services podría permitir que un atacante remoto sin autenticación enviase un paquete modificado, provocando un desbordamiento de búfer o la sobrelectura del mismo, causando la lectura del contenido de la memoria, una denegación de servicio (DoS) o la ejecución de código con nivel de privilegios de root. Se ha reservado el identificador CVE-2018-0304 para esta vulnerabilidad.
- Una vulnerabilidad debida a una insuficiente validación en el procesado de las cabeceras de los paquetes Cisco Fabric Services podría permitir a un atacante remoto sin autenticación generar un paquete modificado que al procesarse provocara un desbordamiento de búfer, pudiendo conllevar a una ejecución de código arbitrario. Se ha reservado el identificador CVE-2018-0314 para esta vulnerabilidad.
- Una vulnerabilidad debida a una insuficiente validación en el procesado de las cabeceras de los paquetes Cisco Fabric Services podría permitir a un atacante remoto sin autenticación generar un paquete modificado que al procesarse provoque un desbordamiento de búfer, conllevando a una ejecución de código arbitrario o a una denegación de servicio (DoS). Se ha reservado el identificador CVE-2018-0312 para esta vulnerabilidad.

Para el resto de vulnerabilidades se han reservado los identificadores: CVE-2018-0307, CVE-2018-0291, CVE-2018-0293, CVE-2018-0292, CVE-2018-0295, CVE-2018-0294, CVE-2018-0330, CVE-2018-0331, CVE-2018-0311, CVE-2018-0310, CVE-2018-0306, CVE-2018-0313, CVE-2018-0299, CVE-2018-0309, CVE-2018-0298, CVE-2018-0302, CVE-2018-0303, CVE-2018-0305, CVE-2018-0300, CVE-2018-0358, CVE-2018-0363, CVE-2018-0364, CVE-2018-0337, CVE-2018-6242, CVE-2018-0365, CVE-2018-0362, CVE-2018-0359, CVE-2018-0373.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en productos de Netgear

Fecha de publicación: 26/06/2018

Importancia: Alta

Recursos afectados:

Las vulnerabilidades publicadas afectan a varios modelos de routers, puertas de enlace y amplificadores de Netgear.

La lista completa de productos afectados se encuentra en la sección *Referencias* mÃis abajo.

Descripción:

Netgear ha publicado soluciones para múltiples vulnerabilidades de severidades alta y media que afectan a varios de sus productos.

Solución:

Descargar la última versión del firmware disponible para cada producto desde la pÃigina web de soporte de Netgear: https://www.netgear.com/support/.

Detalle:

Los tipos de vulnerabilidades solucionadas por Netgear son:

- Configuración de seguridad errónea
- Cross-Site Request Forgery (CSRF)
- Inyección de comandos después de la autenticación
- Desbordamiento de búfer antes y después de la autenticación
- Revelación de información sensible
- Denegación de servicio

Etiquetas: Actualización, Privacidad, Vulnerabilidad

Vulnerabilidades en el gestor de contenidos Joomla!

Fecha de publicación: 27/06/2018

Importancia: Baja

Recursos afectados:

- Joomla! versiones 1.6.0 a la 3.8.8

Descripción:

El gestor de contenidos Joomla! podría ser vulnerable a una inyección XSS o a la realización de una inclusión local de archivos.

Solución:

Actualizar a la última versión:

- Joomla! 3.8.10

Detalle:

- El enlace al idioma actual puede contener caracteres especiales HTML sin filtrar que puede permitir a un atacante realizar un XSS reflejado.
- La función ?class_exists? no realiza las comprobaciones adecuadas pudiendo permitir que un atacante realice una inclusión local de archivos.

Etiquetas: Actualización, Gestor de contenidos, Vulnerabilidad

---

Modificación remota no autorizada en iLO de Hewlett Packard

Fecha de publicación: 27/06/2018

Importancia: Alta

Recursos afectados:

- HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers ? anterior a la v1.30
- HPE Integrated Lights-Out 4 (iLO 4) ? anterior a la v2.60

Descripción:

Hewlett Packard Enterprise (HPE) ha publicado una vulnerabilidad de severidad alta en la que un atacante podría modificar información de manera no autorizada en los productos afectados.

Solución:

HPE ha puesto a disposición de los usuarios las siguientes versiones de firmware que solucionan la vulnerabilidad:

- iLO 4 v2.60
- iLO 5 v1.30

En el sitio https://support.hpe.com/hpesc/public/home, podrÃin descargarse las actualizaciones de firmware.

Detalle:

Un atacante remoto podría explotar una vulnerabilidad en el mecanismo de gestión remota iLO de HP, que podría permitirle modificar información de manera no autorizada. Se ha reservado el identificador CVE-2018-7078 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Múltiples vulnerabilidades en Rational DOORS de IBM

Fecha de publicación: 27/06/2018

Importancia: Alta

Recursos afectados:

- Rational DOORS: 9.5.1 - 9.5.1.9
- Rational DOORS: 9.5.2 - 9.5.2.8
- Rational DOORS: 9.6.0 - 9.6.0.7
- Rational DOORS: 9.6.1 - 9.6.1.10
- Rational DOORS desktop client
- Rational DOORS interoperation server

Descripción:

Se han encontrado tres vulnerabilidades en Rational DOORS, una de severidad alta y dos de severidad media, que podrían causar la obtención de permisos de administración, la recuperación de contraseñas débiles o la denegación del servicio.

Solución:

- Para las versiones de Rational DOORS 9.5.1 - 9.5.1.9, actualizar a la versión 9.5.1.10
- Para las versiones de Rational DOORS 9.5.1 - 9.5.1.9, actualizar a la versión 9.5.2.9
- Para las versiones de Rational DOORS 9.5.1 - 9.5.1.9, actualizar a la versión 9.6.0.8
- Para las versiones de Rational DOORS 9.5.1 - 9.5.1.9, actualizar a la versión 9.6.1.11

Detalle:

- La vulnerabilidad de severidad alta podría permitir a un atacante la obtención de privilegios de administración. Se ha reservado el código CVE-2018-1457 para esta vulnerabilidad.
- La función hash del KDB de GSKit CMS presenta un fallo que conlleva una protección de contraseñas mÃis débil de lo esperado. Un atacante podría aprovechar esta situación para recuperar una contraseña débil. Se ha reservado el código CVE-2018-1447 para esta vulnerabilidad.
- IBM GSKit contiene varias variables de entorno que un atacante podría llegar a desbordar, provocando una denegación de servicio. Se ha reservado el código CVE-2018-1427 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Múltiples vulnerabilidades en varios productos de VMware

Fecha de publicación: 29/06/2018

Importancia: Alta

Recursos afectados:

- VMware vSphere ESXi (ESXi) versiones 14.x
- VMware Workstation Pro / Player (Workstation) versiones14.x
- VMware Fusion Pro, Fusion (Fusion) versiones 10.x

Descripción:

WMware ha publicado múltiples vulnerabilidades de tipo lectura fuera de límites que afectan a sus productos ESXi, Workstation y Fusion, y que podrían desembocar en una divulgación de información o causar un cierre inesperado.

Solución:

Las siguientes actualizaciones estan disponibles:

- ESXi 6.7
- VMware Workstation Pro 14.1.2
- VMware Workstation Player 14.1.2
- VMware Fusion Pro / Fusion 10.1.2

Detalle:

Vulnerabilidades de lectura fuera de límites en el shader traslator podrían permitir la divulgación de información o el cierre inesperado del sistema por usuarios sin privilegios. Se han reservado los identificadores CVE-2018-6965, CVE-2018-6966, y CVE-2018-6967 para estas vulnerabilidades.

Etiquetas: Actualización, VMware, Vulnerabilidad