Alerta de seguridad informática	9VSA-00045-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de agosto de 2019
Última revisión	06 de agosto de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por CISCO referente a vulnerabilidades detectadas en varios de sus productos y sus respectivos parches.

Vulnerabilidad

CVE-2019-12632

Impacto

Una vulnerabilidad en Cisco Finesse podría permitir que un atacante remoto no autenticado omita los controles de acceso y realice un ataque de falsificación de solicitudes del lado del servidor (SSRF) en un sistema afectado.

La vulnerabilidad existe porque el sistema afectado no valida correctamente la entrada proporcionada por el usuario. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud diseñada a un usuario de la aplicación web. Una explotación exitosa podría permitir al atacante acceder al sistema y realizar acciones no autorizadas.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Finesse Software anteriores a 11.6 (1) ES7 o 12.0 (1) ES01.

Mitigación

Aplicar las actualizaciones liberadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-finesse-ssrf

---

Vulnerabilidad

CVE-2019-12644

Impacto

Una vulnerabilidad en la interfaz web del software Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto no autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz de administración web de un dispositivo afectado.

La vulnerabilidad existe porque la interfaz de administración web del dispositivo afectado no valida correctamente la entrada proporcionada por el usuario. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que haga clic en un enlace diseñado. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco ISE Software anteriores a la versión 2.6.0.

Mitigación

Aplicar las actualizaciones liberadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ise-xss

---

Vulnerabilidad

CVE-2019-12645

Impacto

Una vulnerabilidad en Cisco Jabber Client Framework (JCF) Software para Mac, instalada como parte del cliente Cisco Jabber para Mac, podría permitir que un atacante local autenticado ejecute código arbitrario en un dispositivo afectado.

La vulnerabilidad se debe a permisos de nivel de archivo incorrectos en un dispositivo afectado cuando ejecuta el software Cisco JCF para Mac. Un atacante podría aprovechar esta vulnerabilidad autenticándose en el dispositivo afectado y ejecutando código arbitrario o modificando potencialmente ciertos archivos de configuración.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a Cisco JCF para Mac, versiones de software 12.6 (1) y anteriores.

Mitigación

Aplicar las actualizaciones liberadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-jcf-codex

---

Vulnerabilidad

CVE-2019-12635

Impacto

Autorización del software Cisco Content Security Management Appliance (SMA) podría permitir que un atacante remoto autenticado obtenga acceso fuera de alcance al correo electrónico.

La vulnerabilidad existe porque el software afectado no implementa correctamente los controles de permisos de roles. Un atacante podría aprovechar esta vulnerabilidad mediante el uso de un rol personalizado con permisos específicos. Una explotación exitosa podría permitir al atacante acceder a la cuarentena de spam de otros usuarios.

Productos Afectados
En el momento de la publicación, esta vulnerabilidad afectaba a las SMA de Cisco que ejecutaban versiones de software de Cisco SMA anteriores a la versión 12.5.0 y tenían habilitada la función de cuarentena centralizada de virus, virus y cuarentena.

Mitigación
Aplicar las actualizaciones liberadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-sma-info-dis

Vulnerabilidad

CVE-2019-12633

Impacto

Una vulnerabilidad en Cisco Unified Contact Center Express (Unified CCX) podría permitir que un atacante remoto no autenticado omita los controles de acceso y realice un ataque de falsificación de solicitudes del lado del servidor (SSRF) en un sistema de destino.

La vulnerabilidad se debe a la validación incorrecta de la entrada proporcionada por el usuario en el sistema afectado. Un atacante podría aprovechar esta vulnerabilidad enviando al usuario de la aplicación web una solicitud diseñada. Si se procesa la solicitud, el atacante podría acceder al sistema y realizar acciones no autorizadas.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Unified CCX anteriores a 11.6 (2) ES04 o 12.0 (1) SU0.1.

Mitigación

Aplicar las actualizaciones liberadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-unified-ccx-ssrf

---

Vulnerabilidad

CVE-2019-1976

Impacto

Una vulnerabilidad en el componente de servicios "plug-and-play" de Cisco Industrial Network Director (IND) podría permitir que un atacante remoto no autenticado acceda a información confidencial en un dispositivo afectado.

La vulnerabilidad se debe a restricciones de acceso inadecuadas en la interfaz de administración web. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada a un dispositivo afectado. Una explotación exitosa podría permitir al atacante acceder a la información de configuración en ejecución sobre los dispositivos administrados por el IND, incluidas las credenciales administrativas.

Productos Afectados

Las versiones de Cisco IND anteriores a la versión 1.6.0 se ven afectadas cuando los servicios plug-and-play están habilitados. Los servicios Plug-and-play no están habilitados de manera predeterminada.

Mitigación

Aplicar las actualizaciones liberadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ind

---

Vulnerabilidad
CVE-2019-1939

Impacto
Una vulnerabilidad en el cliente Cisco Webex Teams para Windows podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en un sistema afectado.

Esta vulnerabilidad se debe a restricciones inadecuadas en las funciones de registro de software utilizadas por la aplicación en los sistemas operativos Windows. Un atacante podría explotar esta vulnerabilidad al convencer a un usuario objetivo de que visite un sitio web diseñado para enviar información maliciosa a la aplicación afectada. Una explotación exitosa podría permitir que el atacante haga que la aplicación modifique archivos y ejecute comandos arbitrarios en el sistema con los privilegios del usuario objetivo.

Productos Afectados
Esta vulnerabilidad afecta a todas las versiones de Cisco Webex Teams para Windows anteriores a la versión 3.0.12427.0.

Mitigación
Aplicar las actualizaciones liberadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.06 19:24:16 -04'00'