BOLETÍN DE ALERTA

Boletín Nro.: 2022-03

Fecha de publicación: 14/01/2022

Tema: Cisco ha publicado parches de seguridad para sus productos.

Softwares afectados:

- **Cisco Adaptive Security Device Manager versión 7.15.1**
- **Cisco Enterprise Chat and Email versiones anteriores a 12.6(1)_ES1**
- **Cisco IP Phones:**
  - **IP Conference Phone 7832**
  - **IP Conference Phone 8832**
  - **IP Phones 7811, 7821, 7841, and 7861**
  - **IP Phones 8811, 8841,8845, 8851, 8861, and 8865**
  - **Unified IP Conference Phone 8831**
  - **Unified IP Conference Phone 8831 for Third-Party Call Control**
  - **Unified IP Phones 7945G, 7965G, and 7975G**
  - **Unified SIP Phone 3905**
  - **Wireless IP Phones 8821 and 8821-EX**
- **Cisco Prime Access Registrar Appliance versiones anteriores a 9.2.0.0**
- **Cisco Prime Infrastructure and Evolved Programmable Network Manager**
  - **Cisco PI versiones anteriores a 3.10**
  - **Cisco EPNM versiones anteriores a 5.1.3**
- **Cisco Secure Network Analytics versiones anteriores a 7.2.1**
- **Cisco Security Manager versiones anteriores a 4.24**
- **Cisco Tetration versiones anteriores a 3.5.1**
- **Cisco Unified Contact Center Management Portal and Unified Contact Center Domain Manager 12.5.1, 12.0.1 y versiones anteriores a 11.6.1**

Descripción:

Cisco ha publicado parches de seguridad para mitigar múltiples vulnerabilidades como escalamiento de privilegios, *Cross-Site Scripting* (XSS) y divulgación de información entre las más destacadas, que afectarían a sus distintos productos.

La vulnerabilidad más relevante identificada como CVE-2022-20658, de severidad critica, posee una puntuación de 9.6. Ésta se encuentra en la interfaz de administración web de *Cisco Unified Contact Center Management Portal* (Unified CCMP) y *Cisco Unified Contact Center Domain Manager* (Unified CCDM); se debe a una falta de validación del lado del servidor de los permisos de usuario. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP y así lograr un escalamiento de privilegios en el sistema afectado.

Las otras vulnerabilidades encontradas poseen una severidad media, éstas son las siguientes:

- Vulnerabilidades Cross-Site Scripting (XSS) en Cisco Security Manager: Múltiples vulnerabilidades en la interfaz de administración web de *Cisco Security Manager*. Éstas deben en una insuficiente validación de la entrada proporcionada por el usuario, esto permitiría que un atacante realice ataques de *Cross-Site Scripting* (XSS). Éstas vulnerabilidades se encuentran asociadas a los siguientes identificadores: CVE-2022-20635, CVE-2022-20636, CVE-2022-20637, CVE-2022-20638, CVE-2022-20639, CVE-2022-20640, CVE-2022-20641, CVE-2022-20642, CVE-2022-20643, CVE-2022-20644, CVE-2022-20645, CVE-2022-20646 y CVE-2022-20647. Para más información ingresar al siguiente enlace.

- Vulnerabilidades en Cisco Enterprise Chat and Email: Múltiples vulnerabilidades en la interfaz de administración web de *Cisco Enterprise Chat and Email* (ECE). Éstas se deben a que una incorrecta validación en la entrada proporcionada por el usuario, esto permitiría a un atacante remoto no autenticado realizar ataques de *Cross-Site Scripting* (XSS), enumerar cuentas de usuarios existentes y redirigir a un usuario a una página web no deseada. Éstas vulnerabilidades se encuentran asociadas a los siguientes identificadores: CVE-2022-20631, CVE-2022-20632, CVE-2022-20633 y CVE-2022-20634. Para más información ingresar al siguiente enlace.

- Vulnerabilidad de divulgación de información en teléfonos IP Cisco: Una vulnerabilidad en la arquitectura de almacenamiento de información en varios modelos de *Cisco IP Phone*. Ésta vulnerabilidad se debe al almacenamiento sin cifrar de la información confidencial en el dispositivo afectado, esto permitiría a un atacante físicamente y sin autenticarse obtenga información confidencial del dispositivo afectado. Ésta vulnerabilidad se encuentra asociada al identificador CVE-2022-20660. Para más información ingresar al siguiente enlace.

- Vulnerabilidades en Cisco Prime Infrastructure y Evolved Programmable Network Manager: Múltiples vulnerabilidades en la interfaz de administración web de *Cisco Prime Infrastructure* (PI) y *Cisco Evolved Programmable Network Manager* (EPNM). Estas vulnerabilidades se deben a una validación insuficiente en la entrada proporcionada por el usuario, esto permitiría a un atacante realizar ataques de *path traversal* y *Cross-Site Scripting* (XSS). Éstas vulnerabilidades se encuentran asociadas a los siguientes identificadores: CVE-2022-20656 y CVE-2022-20657. Para más información ingresar al siguiente enlace.

- Vulnerabilidad Cross-Site Scripting (XSS) en Cisco Prime Access Registrar: Una vulnerabilidad en la interfaz de administración web de *Cisco Prime Access Registrar* (PAR). Esta vulnerabilidad se debe a una validación insuficiente en la entrada proporcionada por el usuario, esto permitiría a un atacante realizar *Cross-Site Scripting* (XSS) y se encuentra asociada al identificador CVE-2022-20626. Para más información ingresar al siguiente enlace.

- Vulnerabilidad Cross-Site Scripting (XSS) en Cisco Secure Network Analytics: Una vulnerabilidad en la interfaz de administración web de *Cisco Secure Network Analytics*, anteriormente *Stealthwatch Enterprise*. Esta vulnerabilidad se debe a una validación insuficiente en la entrada proporcionada por el usuario, esto permitiría a un atacante realizar *Cross-Site Scripting* (XSS) y se encuentra asociada al identificador CVE-2022-20663. Para más información ingresar al siguiente enlace.

- Vulnerabilidad de inyección de comandos en Cisco Tetration: Una vulnerabilidad en la interfaz de web y el subsistema *API* de *Cisco Tetration*. Esta vulnerabilidad se debe a una validación insuficiente en la entrada proporcionada por el usuario, un atacante podría aprovechar esta vulnerabilidad enviando un mensaje *HTTP* malicioso al sistema afectado. Esto podría permitir a un atacante remoto autenticado inyectar comandos para ejecutarlos con privilegios a nivel de *root* en el sistema operativo. Ésta vulnerabilidad se encuentra asociada al identificador CVE-2022-20652. Para más información ingresar al siguiente enlace.

- Vulnerabilidad de divulgación de información en Cisco Adaptive Security Device Manager: Una vulnerabilidad en el componente *logging* de *Cisco Adaptive Security Device Manager* (ASDM). Esta vulnerabilidad se debe al almacenamiento de credenciales sin cifrar en ciertos *logs,* un atacante podría aprovechar esta vulnerabilidad accediendo a los *logs* del sistema afectado y se encuentra asociada al identificador CVE-2022-20651. Para más información ingresar al siguiente enlace.

Impacto:

Un atacante podría realizar escalamiento de privilegios o ejecución remota de código (RCE) y así obtener control total de los diferentes productos Cisco.

Solución:

Recomendamos instalar las actualizaciones de seguridad correspondientes al producto utilizado afectado a través del siguiente enlace:

- https://www.cisco.com/c/en/us/support/index.html

Información adicional:

- https://www.govcert.gov.hk/en/alerts_detail.php?id=719
- https://www.cisa.gov/uscert/ncas/current-activity/2022/01/13/cisco-releases-security-updates-multiple-products
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-logging-jnLOY422
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-priv-esc-JzhTFLm4
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-mult-xss-7hmOKQTt
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-multivulns-kbK2yVhR
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-info-disc-fRdJfOxA
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-path-trav-zws324yn
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-reg-xss-zLOz8PfB
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-NXOxDhRQ
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tetr-cmd-injc-skrwGO