BOLETÍN DE ALERTA

Boletín Nro.: 2020-05

Fecha de publicación: 12/02/2020

Tema: Actualizaciones de seguridad en productos Cisco abordan múltiples vulnerabilidades.

- Las vulnerabilidades declaradas como críticas, son: CVE-2020-3120, CVE-2020-3119, CVE-2020-3118, CVE-2020-3111 y CVE-2020-3110.
- Además, existen vulnerabilidades que han sido declaradas con criticidad media: CVE-2020-3149 y CVE-2019-15253

Sistemas afectados:

- Afecta a los siguientes productos de Cisco, si tienen el protocolo "Cisco Discovery" habilitado, tanto a nivel global como en al menos una interfaz y si están ejecutando una versión vulnerable de:
    - En el CVE-2020-3120, versión vulnerable del software Cisco **FXOS**, **IOS XR (32-bit or 64-bit)** o **NX-OS** en:
        - ASR 9000 Series Aggregation Services Routers
        - Carrier Routing System (CRS)
        - Firepower 4100 Series
        - Firepower 9300 Security Appliances
        - IOS XRv 9000 Router
        - MDS 9000 Series Multilayer Switches
        - Network Convergence System (NCS) 540 Series Routers
        - Network Convergence System (NCS) 560 Series Routers
        - Network Convergence System (NCS) 1000 Series
        - Network Convergence System (NCS) 5000 Series
        - Network Convergence System (NCS) 5500 Series
        - Network Convergence System (NCS) 6000 Series
        - Nexus 1000 Virtual Edge for VMware vSphere
        - Nexus 1000V Switch for Microsoft Hyper-V
        - Nexus 1000V Switch for VMware vSphere
        - Nexus 3000 Series Switches

- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in standalone NX-OS mode
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

○ En el CVE-2020-3119, versión vulnerable del software Cisco **NX-OS** en:

- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in standalone NX-OS mode

○ En el CVE-2020-3118, versión vulnerable del software Cisco **IOS XR en:**

- ASR 9000 Series Aggregation Services Routers
- Carrier Routing System (CRS)
- IOS XRv 9000 Router
- Network Convergence System (NCS) 540 Series Routers
- Network Convergence System (NCS) 560 Series Routers
- Network Convergence System (NCS) 1000 Series Routers
- Network Convergence System (NCS) 5000 Series Routers
- Network Convergence System (NCS) 5500 Series Routers
- Network Convergence System (NCS) 6000 Series Routers

- El CVE-2020-3111, versión vulnerable de firmware en teléfonos IP CISCO:
  - IP Conference Phone 7832
  - IP Conference Phone 7832 con firmware multiplataforma.
  - IP Conference Phone 8832
  - IP Conference Phone 8832 con firmware multiplataforma.
  - IP Phone 6821, 6841, 6851, 6861, 6871 con firmware multiplataforma.
  - IP Phone 7811, 7821, 7841, 7861 Desktop Phones
  - IP Phone 7811, 7821, 7841, 7861 Desktop Phones con firmware multiplataforma.
  - IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones
  - IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones con firmware multiplataforma.
  - Unified IP Conference Phone 8831
  - Unified IP Conference Phone 8831 for Third-Party Call Control
  - Wireless IP Phone 8821, 8821-EX

- En el CVE-2020-3110, afecta a las cámaras IP de Cisco Video Surveillance serie 8000 que ejecutan una versión de firmware anterior a la 1.0.7.

- El CVE-2020-3149, afecta a las versiones del software Cisco **ISE** anteriores a la 2.7.0.

- El CVE-2019-15253, afecta a las versiones del software Cisco **DNA** Center anteriores a la 1.3.0.6 y la 1.3.1.4.

Descripción:

Recientemente Cisco ha publicado una serie de avisos de seguridad donde se informa la corrección de múltiples vulnerabilidades. Los CVE-2020-3120, CVE-2020-3111 y CVE-2020-3110 podrían permitir a un atacante no autenticado provocar un ataque de denegación de servicio **(DoS)**. La misma se da debido a la falta de verificación cuando se procesan los mensajes del protocolo de descubrimiento de Cisco **(Cisco Discovery Protocol)**, con esto un atacante podría enviar un paquete malicioso del Cisco Discovery Protocol a un dispositivo afectado, agotar la memoria del sistema y lograr que el dispositivo se recargue.

Los CVE-2020-3119 y CVE-2020-3118, describen una vulnerabilidad que podría permitir a un atacante no autenticado la ejecución remota de código con privilegios administrativos en los dispositivos afectados. La vulnerabilidad se da debido a que analizador del Cisco Discovery Protocol no valida correctamente la entrada para ciertos campos en un mensaje del mismo, con esto un atacante podría enviar un paquete malicioso de Cisco Discovery Protocol a un dispositivo afectado, causar un desbordamiento de la pila y lograr la ejecución de código remoto.

En cuanto al CVE-2020-3149, describe una vulnerabilidad que podría permitir a un atacante remoto autenticado realizar ataques de Cross-Site-Scripting **(XSS)** almacenado en los dispositivos afectados. La vulnerabilidad se da debido validación de entrada insuficiente por parte de la interfaz de administración basada en web de Cisco Identity Services Engine **(ISE)**. La explotación exitosa de esta vulnerabilidad podría permitir al atacante ejecutar código malicioso en la interfaz afectada o acceder a información confidencial del navegador.

Por último, el CVE-2019-15253, podría permitir a un atacante remoto autenticado realizar ataques de Cross-Site-Scripting **(XSS)** almacenado en los dispositivos afectados. La vulnerabilidad se da debido validación de entrada insuficiente por parte de la interfaz de administración basada en web del Centro de arquitectura de red digital **(DNA)**. La explotación exitosa de esta vulnerabilidad podría permitir al atacante ejecutar código malicioso en la interfaz afectada o acceder a información confidencial del navegador, cabe destacar que para la explotación de esta vulnerabilidad un atacante necesita credenciales de administrador.

Según el centro de respuestas ante incidentes de cisco (PSIRT) no existen pruebas de que estas vulnerabilidades han sido explotadas.

Solución y Prevención

Cisco ha lanzado actualizaciones de software gratuitas que abordan la vulnerabilidad descrita. Los clientes solo pueden instalar y esperar soporte para versiones de software para los que han comprado una licencia. Se recomienda su actualización en los dispositivos afectados:

- Para el **CVE-2020-3120**:

- La lista de actualizaciones para cada dispositivo afectado se puede ver y descargar en la sección de Fixed Software.
- Además como solución alternativa, se recomienda:
  - Verificar el estado del protocolo "Cisco Discovery" (ver los pasos a seguir para cada dispositivo en la sección "Status of Cisco Discovery Protocol" aquí), y en caso de estar habilitado y no hacer uso del mismo,
  - deshabilitar de acuerdo a al dispositivo utilizado, puede ver los pasos en la sección "Workaround" aquí.

- Para el CVE-2020-3119:
  - La lista de actualizaciones para cada dispositivo afectado se puede ver y descargar en la sección de Fixed Software.
  - Además como solución alternativa, se recomienda:
    - Verificar el estado del protocolo "Cisco Discovery" (ver los pasos a seguir para cada dispositivo en la sección "Status of Cisco Discovery Protocol" aquí), y en caso de estar habilitado, y no hacer uso del mismo,
    - deshabilitar de acuerdo al dispositivo utilizado, puede ver los pasos en la sección "Workaround" aquí.

- Para el CVE-2020-3118:
  - La lista de actualizaciones para cada dispositivo afectado se puede ver y descargar en la sección de Fixed Software.
  - Además como solución alternativa, se recomienda:
    - Verificar el estado del protocolo "Cisco Discovery" (ver en la sección "Status of Cisco Discovery Protocol" aquí), y en caso de estar habilitado y no hacer uso del mismo,

- deshabilitar, de acuerdo al dispositivo utilizado puede ver los pasos en la sección “Workaround” aquí.

- Para el CVE-2020-3111:
  - La lista de actualizaciones para cada dispositivo afectado se puede ver y descargar en la sección de Fixed Software.
- Para el CVE-2020-3110:
  - Actualizar el Firmware de la cámara IP de Cisco Video Surveillance serie 8000 a 1.0.7 y posteriores, desde aquí.
- Para el CVE-2020-3149:
  - Actualizar Cisco ISE Software versiones 2.7.0 y posteriores, desde aquí.
- Para el CVE-2019-15253:
  - Actualizar el Centro de arquitectura de red digital (DNA) a 1.3.0.6 y posteriores o 1.3.1.4 y posteriores, desde desde aquí.

Información adicional:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-DxJsRWRx
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190205-dnac-xss