Cisco ha lanzado parches de seguridad para abordar múltiples vulnerabilidades de seguridad, incluyendo una falla crítica, que podría ser aprovechada por un actor malicioso para tomar el control de un sistema afectado o provocar una condición de denegación de servicio (DoS).

La más grave de estas cuestiones es el CVE-2023-20238, que tiene la calificación de severidad máxima en el sistema CVSS, con una puntuación de 10.0. Esta vulnerabilidad se describe como un fallo de omisión de autenticación en la Plataforma de Entrega de Aplicaciones Cisco BroadWorks y la Plataforma de Servicios Extendidos Cisco BroadWorks.

La explotación exitosa de esta vulnerabilidad, que se detectó durante pruebas internas y se relaciona con una debilidad en la implementación de inicio de sesión único (SSO), podría permitir a un atacante remoto no autenticado falsificar las credenciales necesarias para acceder a un sistema afectado.

> Cisco explicó: *«Esta vulnerabilidad se debe al método utilizado para validar los tokens de SSO. Un atacante podría explotar esta vulnerabilidad autenticándose en la aplicación con credenciales falsificadas. Si tiene éxito, el atacante podría cometer fraude telefónico o ejecutar comandos con el nivel de privilegio de la cuenta falsificada. Si esa cuenta es de administrador, el atacante tendría la capacidad de acceder a información confidencial, modificar la configuración de clientes o alterar la configuración de otros usuarios. Para explotar esta vulnerabilidad, el atacante necesitaría disponer de un ID de usuario válido asociado a un sistema Cisco BroadWorks afectado».*

Esta vulnerabilidad afecta a ambos productos BroadWorks y requiere que una de las siguientes aplicaciones esté habilitada: AuthenticationService, BWCallCenter, BWReceptionist, CustomMediaFilesRetrieval, ModeratorClientApp, PublicECLQuery, PublicReporting, UCAPI, Xsi-Actions, Xsi-Events, Xsi-MMTel o Xsi-VTR.

Las correcciones para esta vulnerabilidad están disponibles en las siguientes versiones: AP.platform.23.0.1075.ap385341, 2023.06_1.333 y 2023.07_1.332.

Cisco también ha solucionado un defecto de alta severidad en la característica de procesamiento de mensajes RADIUS de Cisco Identity Services Engine (CVE-2023-20243, con una puntuación CVSS de 8.6) que podría permitir a un atacante remoto no autenticado causar que el sistema afectado deje de procesar paquetes RADIUS.

> La empresa explicó: *«Esta vulnerabilidad se debe a un manejo inadecuado de ciertas solicitudes de contabilidad RADIUS. Un ataque exitoso podría hacer que el proceso RADIUS se reinicie de manera inesperada, lo que resultaría en tiempos de autenticación o autorización agotados y negaría el acceso a la red o al servicio a usuarios legítimos».*

El CVE-2023-20243 afecta a las versiones 3.1 y 3.2 de Cisco Identity Services Engine y ha sido corregido en las versiones 3.1P7 y 3.2P3. Las otras versiones del producto no son susceptibles.

Juniper Networks Aborda una Vulnerabilidad Grave en BGP con una Actualización Fuera de Banda

Estas advertencias llegan poco después de que Juniper Networks lanzara una actualización fuera de banda para una vulnerabilidad de validación de entrada inadecuada en el Demonio de Protocolo de Enrutamiento (rpd) de Junos OS y Junos OS Evolved, que permite a un atacante de red no autenticado provocar una condición de DoS.

La vulnerabilidad afecta a varias implementaciones del Protocolo de Puerta de Enlace Fronteriza (BGP), según el investigador de seguridad Ben Cartwright-Cox, quien descubrió el problema. Juniper Networks la ha registrado como CVE-2023-4481 (con una puntuación CVSS de 7.5), FRRouting como CVE-2023-38802 y OpenBSD OpenBGPd como CVE-2023-38283.

> Juniper Networks explicó: *«Cuando se reciben ciertos mensajes BGP UPDATE*

> *específicos y manipulados a través de una sesión BGP establecida, una sesión BGP puede cerrarse con un error de mensaje UPDATE, o el problema puede propagarse más allá del sistema local, que permanecerá sin verse afectado, pero puede afectar a uno o varios sistemas remotos».*

> *«Esta problemática puede ser aprovechada de forma remota ya que el mensaje UPDATE modificado puede propagarse a través de sistemas no afectados y oradores BGP intermedios. La recepción constante de los mensajes BGP UPDATE modificados creará una condición de denegación de servicio (DoS) continua para los dispositivos afectados».*

No obstante, para que el ataque tenga éxito, se requiere que un atacante remoto tenga al menos una sesión BGP establecida. La vulnerabilidad ha sido corregida en Junos OS 23.4R1 y Junos OS Evolved 23.4R1-EVO.

Vulnerabilidad no parcheada en el router módem Tenda

En un desarrollo relacionado, el Centro de Coordinación CERT (CERT/CC) detalló una vulnerabilidad de omisión de autenticación no corregida en el router módem Tenda N300 Wireless N VDSL2 (CVE-2023-4498) que permite a un usuario remoto no autenticado acceder a información delicada mediante una solicitud especialmente diseñada.

> *«La explotación exitosa de esta vulnerabilidad podría otorgar al atacante acceso a páginas que, de otra manera, requerirían autenticación. Un atacante no autenticado podría obtener acceso a información confidencial, como la contraseña administrativa, que podría ser utilizada para llevar a cabo ataques adicionales»,* mencionó CERT/CC.

En ausencia de una actualización de seguridad, se aconseja a los usuarios desactivar tanto los servicios de administración remota (lado WAN) como la interfaz web en el WAN en cualquier router SoHo.