"Rastreando la Vulnerabilidad: Un Relato de Seguridad en Redes Corporativas"

La convocatoria de reunión extraordinaria de anoche ya presagiaba malas noticias. Hoy, 17 de octubre de 2023, la dirección nos informó de que nuestros sistemas CISCO se han visto afectados por una vulnerabilidad crítica con nombre propio: la CVE-2023-20198.

Aunque no soy experta en ciberseguridad, la responsabilidad recae en nuestro equipo para investigar y abordar esta situación. No puedo evitar recordar ese congreso al que asistimos hace unos meses, donde se resaltaba cómo las vulnerabilidades zero-day estaban a la orden del día. Creímos que eso solo afectaba a grandes empresas, ¡qué ingenuos!.

Lo primero que salta a la vista, es la gravedad de la vulnerabilidad. Permite a un atacante remoto tomar el control de nuestros sistemas, otorgando un nivel de privilegio 15. Busco entre los niveles de autorización de comandos de CISCO y leo: “Incluye todos los comandos del permiso-nivel en el prompt del router”. Nos explican que la vulnerabilidad está siendo explotada para crear cuentas de usuario y, posteriormente, elevar los privilegios hasta el nivel de root. Esto es un golpe duro, considerando que confiamos en la robustez de la tecnología CISCO. Los datos de nuestros proyectos y clientes, quedan a unos pocos comandos y clicks de extraños: ¡Menuda locura!

Después del primer impacto y tras comprender la magnitud del problema, toca ser rápidos. Se ha emitido una recomendación urgente de desactivar el servidor HTTP en todos los sistemas con acceso a Internet. Pero aquí surge mi primera pregunta: ¿cómo afectará esto a nuestras operaciones diarias? Habrá que recurrir a soluciones temporales mientras abordamos la vulnerabilidad: Información actualizada a usuarios, página de mantenimiento, redirección del tráfico para mantener la continuidad de algunas operaciones críticas,...

La información técnica proporcionada por CISCO es abrumadora para alguien sin un fondo técnico profundo, pero puedo identificar algunas acciones clave. La actualización a la última versión es esencial, y aquí es donde me doy cuenta de la importancia de contar con contratos de servicio que brindan derecho a actualizaciones periódicas de software. Afortunadamente, en nuestra empresa, contamos con esos contratos, lo cual es un alivio.

Las medidas de mitigación, como desactivar el servidor HTTP y limitar el acceso a redes confiables, son sugerencias prácticas que podemos comenzar a implementar, aunque siento la presión de la urgencia. Además, la recomendación de monitorear activamente la red en busca de posibles indicadores de compromiso resuena en mi mente (con la voz de mi analista).

En momentos como este, donde la preocupación aumenta a cada momento, me doy cuenta de la necesidad de una comunicación clara con el equipo y la alta dirección. Coordinarnos a su vez, con el Centro de Asistencia Técnica (TAC) de CISCO parece ser un paso lógico para obtener orientación y soporte adicional. En poco tiempo, nos encontramos investigando herramientas como Snort y comandos como curl para verificar la presencia de

implantes en nuestros sistemas. Cada paso es crucial, y aunque no dispongo de toda la experiencia técnica, siento que aprendo rápidamente sobre la marcha.

Esta situación destaca la importancia de la ciberseguridad y la necesidad de mantenerse actualizado con las buenas prácticas. En estas situaciones, hay que actuar con determinación, seguir las recomendaciones proporcionadas, y trabajar en estrecha colaboración con los expertos para restaurar la integridad de nuestros sistemas. La lección aprendida es que, la responsabilidad de la seguridad cibernética es un desafío que todos debemos enfrentar y abordar de manera proactiva, independientemente del nivel de experticia.

Referencias consultadas:

1. https://www.incibe.es/incibe-cert/alerta-temprana/avisos/escalada-de-privilegios-de-la-interfaz-en-cisco-ios-xe
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
3. https://www.ciberseguridad.eus/ultima-hora/vulnerabilidades-de-alta-gravedad-en-productos-cisco
4. https://unaaldia.hispasec.com/2023/10/cisco-advierte-sobre-una-vulnerabilidad-zero-day-critica-en-el-software-ios.html
5. https://www.cisco.com/c/es_mx/support/docs/security/secure-access-control-server-unix/4104-8.html