Investigadores de seguridad cibernética revelaron el miércoles una nueva vulnerabilidad de derivación (CVE-2021-23008) en la función de seguridad del Centro de Distribución de Claves de Kerberos (KDC), que afecta a los servicios de entrega de aplicaciones F5 Big-IP.

> *«La vulnerabilidad de suplantación de KDC permite a un atacante eludir la autenticación Kerberos en Big-IP Access Policy Manager (APM), eludir las políticas de seguridad y obtener acceso sin restricciones a cargas de trabajo sensibles. En algunos casos, esto también se puede utilizar para omitir la autenticación en la consola de administración de Big-IP»,* dijeron los investigadores de Silverfort, Yaron Kassner y Rotem Zach.

Al tiempo de la divulgación pública, F5 lanzó un parche para abordar la vulnerabilidad.

Kerberos es un protocolo de autenticación que se basa en un modelo cliente-servidor para la autenticación mutua y requiere un intermediario confiable llamado Centro de Distribución de Claves (KDC), un servidor de autenticación Kerberos (AS) o un servidor de concesión de tickets en este caso, que actúa como un repositorio de claves secretas compartidas de todos los usuarios, así como información sobre qué usuarios tienen privilegios de acceso a qué servicios en qué servidores de red.

Por lo tanto, cuando un usuario quiere acceder a un servicio en particular en un servidor, se le pide al usuario que proporcione su nombre de usuario y contraseña para verificar su identidad, después de lo cual el AS verifica si el usuario tiene privilegios de acceso al servidor, y si los tiene, emitir un «ticket» que permita al usuario utilizar el servicio hasta su fecha de vencimiento.

> *«Un atacante remoto puede secuestrar una conexión KDC mediante una respuesta AS-REP falsificada. Pero una política de acceso APM configurada con autenticación AD y agente SSO (inicio de sesión único), si se utiliza una credencial falsificada relacionada con esta vulnerabilidad, según como el sistema back-end valida el*

> *token de autenticación que recibe, el acceso probablemente fallará. También se puede configurar una política de acceso de APM para la autenticación del sistema BIG-IP. Una credencial falsificada relacionada con esta vulnerabilidad para un usuario administrativo a través de la política de acceso de APM da como resultado un acceso administrativo local»,* dijo F5 en un aviso.

También es esencial como parte del proceso la autenticación de KDC en el servidor, en cuyo caso la seguridad de Kerberos se ve comprometida, lo que permite que un atacante tenga la capacidad de secuestrar la comunicación de red entre BIG-IP y el controlador de dominio para eludir la autenticación por completo.

En otras palabras, la idea es que cuando el protocolo Kerberos se implementa de la forma correcta, un adversario que intenta hacerse pasar por el KDC no puede eludir las protecciones de autenticación. El ataque de suplantación, por lo tanto, depende de la posibilidad de que existan configuraciones Kerberos inseguras para secuestrar la comunicación entre el cliente y el controlador de dominio, aprovechándola para crear un KDC fraudulento que desvía el tráfico destinado al controlador al KDC falso y posteriormente autenticarse ante el cliente.

Esta es la cuarta vulnerabilidad de suplantación de identidad descubierta por Silverfort después de descubrir problemas similares en Cisco ASA (CVE-2020-3125), Palo Alto Networks PAN-OS (CVE-2020-2002) e IBM QRadar (CVE-2019-4545).