Cisco está pidiendo a sus clientes que actualicen su software Firepower Management Center, después de que los investigadores informaron sobre una vulnerabilidad crítica que los hackers podrían explotar en Internet.

Como muchos errores de Cisco, la falla se encontró en la interfaz de administración basada en la web de su software. El error tiene una calificación de severidad de 9.8 de 10, lo que significa que los administradores deben parchear lo más pronto posible.

La vulnerabilidad es causada por una falla en la forma en que el software de Cisco maneja las respuestas de autenticación del Protocolo Ligero de Acceso a Directorios (LDAP), desde un servidor de autenticación externo. Los atacantes remotos podrían explotar la falla enviando solicitudes HTTP especialmente diseñadas al dispositivo.

Los dispositivos son vulnerables si se han configurado para autenticar a los usuarios de la interfaz web por medio de un servidor LDAP externo. La compañía de redes recomienda que los administradores vayan a Sistema>Usuarios>Autenticación externa, para ver si se ha configurado para la autenticación LDAP externa.

La forma en que los clientes deben solucionar el problema dependerá de la versión de Firepower Management Center (FMC) que estén ejecutando. No existe una solución alternativa, pero hay parches de revisión disponibles para distintas versiones nuevas de FMC, y las versiones de mantenimiento que abordan la falla están programadas para finales del año.

> *«Los clientes pueden instalar una solución ya sea actualizando a una versión fija o instalando un parche de revisión»,* dijo Cisco.

La compañía también recomienda que los clientes en FMC anterior a 6.1.0, que ya no son compatibles, migren a una versión compatible.

Los clientes de 6.2.0, 6.2.1 y 6.2.2, deben migrar a una nueva versión, como la 6.2.3 de FMC,

que cuenta con un parche disponible y verá una versión de mantenimiento en febrero, mientras que se lanzará una versión de mantenimiento para sistemas en la versión 6.3.0 en mayo de 2020. La versión 6.3.0 también tiene un parche ya disponible.

Los clientes de FMC versión 6.4.0 deben aplicar parches o actualizar a la versión 6.4.0.7, mientras que los clientes de FMC 6.5.0 deben actualizar a 6.5.0.2.

Cisco recomienda que los clientes en versiones anteriores a la 6.1.0 pasen a la 6.2.3 y apliquen los parches. Aquellos en 6.1.0 deben aplicar el hotfix o pasar a 6.2.3 y luego aplicar el hotfix.

Este error crítico no afecta al software del dispositivo de seguridad adaptable de Cisco (ASA) ni al software de defensa contra amenazas Cisco Firepower.