Cisco lanzó el miércoles parches para 10 vulnerabilidades de seguridad que abarcan múltiples productos, una de las cuales, está clasificada como crítica en nivel de gravedad y podría usarse como arma para realizar ataques transversales absolutos.

Las vulnerabilidades, rastreadas como CVE-2022-20812 y CVE-2022-20813, afectan a Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) y *«podrían permitir que un atacante remoto sobrescriba archivos arbitrarios o realice ataques de envenenamiento de bytes nulos en un servidor afectado»,* dijo la compañía.

CVE-2022-20812, con puntaje CVSS de 9.0, que se refiere a un caso de sobrescritura arbitraria de archivos en la API de la base de datos del clúster, requiere que el atacante remoto autenticado tenga privilegios de administrador de lectura y escritura en la aplicación para poder montar la ruta de ataques transversales como usuario root.

> *«Esta vulnerabilidad se debe a una validación de entrada insuficiente de los argumentos de comando proporcionados por el usuario. Un atacante podría explotar esta vulnerabilidad al autenticarse en el sistema como un usuario administrativo de lectura y escritura y enviar una entrada manipulada al comando afectado»,* dijo la compañía.

La explotación exitosa de la vulnerabilidad podría permitir al atacante sobrescribir archivos arbitrarios en el sistema operativo subyacente.

CVE-2022-20813 (puntaje CVSS; 7.4), por otro lado, se describe como una falla de envenenamiento de bytes nulos que surge debido a una validación incorrecta del certificado, que un atacante podría usar como arma para organizar un ataque de intermediario (MitM) y obtener acceso no autorizado a datos confidenciales.

Cisco también parchó una vulnerabilidad de alta gravedad en su Smart Software Manager On-Prem (CVE-2022-20808, puntuación CVSS: 7.7) que podría ser abusada por un atacante remoto autenticado para causar una condición de denegación de servicio (DoS) en un

dispositivo afectado.

Fortinet lanza correcciones para varios de sus productos

En un desarrollo similar, Fortinet abordó hasta cuatro vulnerabilidades de alta gravedad que afectan a FortiAnalyzer, FortiClient, FortiDeceptor y FortiNAC:

- CVE-2021-43072 (puntuación CVSS: 7.4): Desbordamiento de búfer basado en pila por medio del comando de ejecución CLI diseñado en FortiAnalyzer, FortiManager, FortiOS y FortiProxy.
- CVE-2021-41031 (puntuación CVSS: 7.8): Escalada de privilegios a través de un ataque transversal de directorio en FortiClient para Windows
- CVE-2022-30302 (puntaje CVSS: 7.9): Vulnerabilidades transversales de múltiples rutas en la interfaz de administración de FortiDeceptor
- CVE-2022-26117 (puntaje CVSS: 8.0): Cuenta raíz de MySQL desprotegida en FortiNAC

Si las vulnerabilidades se explotan exitosamente, podrían permitir que un atacante autenticado ejecute código arbitrario, recupere y elimine archivos y acceda a bases de datos MySQL, o incluso permitir que un atacante local sin privilegios escale a permisos de SYSTEM.