Cisco ha lanzado actualizaciones para corregir una vulnerabilidad de máxima severidad que afecta a Smart Software Manager On-Prem (Cisco SSM On-Prem), la cual podría permitir a un atacante remoto no autenticado cambiar la contraseña de cualquier usuario, incluidos los administrativos.

La vulnerabilidad, identificada como CVE-2024-20419, tiene una puntuación CVSS de 10.0.

> *«Esta vulnerabilidad se debe a una implementación inadecuada del proceso de cambio de contraseña. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP manipuladas a un dispositivo afectado. Una explotación exitosa permitiría al atacante acceder a la interfaz web o API con los privilegios del usuario comprometido»,* dijo la compañía en un comunicado.

El problema afecta a las versiones 8-202206 y anteriores de Cisco SSM On-Prem. Se ha corregido en la versión 8-202212. Cabe destacar que la versión 9 no presenta esta falla.

Cisco indicó que no existen soluciones alternativas que resuelvan el problema y que no tiene conocimiento de explotación maliciosa activa. El investigador de seguridad Mohammed Adel ha sido acreditado con el descubrimiento y reporte del error.

Otra vulnerabilidad crítica de escritura de archivos en Secure Email Gateway (CVE-2024-20401, puntuación CVSS: 9.8) también ha sido corregida por el fabricante de equipos de red. Esta falla permite a los atacantes agregar nuevos usuarios con privilegios de root y bloquear permanentemente los dispositivos mediante correos electrónicos con archivos adjuntos maliciosos.

«Un atacante podría explotar esta vulnerabilidad enviando un correo electrónico que contenga un archivo adjunto manipulado a través de un dispositivo afectado. Una explotación exitosa permitiría al atacante reemplazar cualquier archivo en el sistema de archivos subyacente», se indicó.

> *«El atacante podría realizar cualquiera de las siguientes acciones: agregar usuarios con privilegios de root, modificar la configuración del dispositivo, ejecutar código arbitrario o causar una denegación de servicio (DoS) permanente en el dispositivo afectado.»*

La falla afecta a los dispositivos SEG si están ejecutando una versión vulnerable de Cisco AsyncOS y si se cumplen los siguientes requisitos:

- La función de análisis de archivos (parte de Cisco Advanced Malware Protection) o la función de filtro de contenido está habilitada y asignada a una política de correo entrante.
- La versión de Content Scanner Tools es anterior a 23.3.0.4823.

Un parche para CVE-2024-20401 está disponible a través de las versiones del paquete Content Scanner Tools 23.3.0.4823 y posteriores, que se incluye por defecto en Cisco AsyncOS para Cisco Secure Email Software versiones 15.5.1-055 y posteriores.

CISA añade 3 fallas al catálogo KEV

La divulgación se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) añadió tres vulnerabilidades a su catálogo de Vulnerabilidades Conocidas y Explotadas (KEV), basado en evidencia de explotación activa:

- CVE-2024-34102 (puntuación CVSS: 9.8) – Vulnerabilidad de Restricción Incorrecta de Referencia de Entidad Externa XML (XXE) en Adobe Commerce y Magento Open Source.
- CVE-2024-28995 (puntuación CVSS: 8.6) – Vulnerabilidad de Traversal de Ruta en SolarWinds Serv-U.
- CVE-2022-22948 (puntuación CVSS: 6.5) – Vulnerabilidad de Permisos de Archivo Predeterminados Incorrectos en VMware vCenter Server.

CVE-2024-34102, también conocida como CosmicSting, es una grave falla de seguridad que surge de la gestión incorrecta de la deserialización anidada, permitiendo a los atacantes ejecutar código remotamente. A finales del mes pasado, Assetnote lanzó una prueba de concepto (PoC) de explotación para esta falla.

Los informes sobre la explotación de CVE-2024-28995, una vulnerabilidad de traversal de directorios que podría permitir el acceso a archivos sensibles en la máquina host, fueron detallados por GreyNoise, incluyendo intentos de leer archivos como /etc/passwd.

El abuso de CVE-2022-22948 ha sido atribuido por Mandiant, propiedad de Google, a un grupo de ciberespionaje chino conocido como UNC3886, que tiene un historial de aprovechar vulnerabilidades de día cero en dispositivos Fortinet, Ivanti y VMware.

Las agencias federales deben aplicar las mitigaciones según las instrucciones del proveedor antes del 7 de agosto de 2024 para proteger sus redes contra amenazas activas.