Se descubrieron dos vulnerabilidades graves en el marco de configuración de código abierto SaltStack Sat, que podría permitir a un hacker ejecutar código arbitrario en servidores remotos implementados en centros de datos y entornos de nube.

Los investigadores de F-Secure identificaron las vulnerabilidades a inicio de marzo y se revelaron el jueves, un día después de que SaltStack lanzara un parche (versión 3000.2), que aborda los problemas, con un puntaje CVSS de 10.

> *«Las vulnerabilidades, con identificadores CVE asignados como CVE-2020-11651 y CVE-2020-11652, son de dos clases diferentes»,* dijo la compañía de seguridad cibernética.
>
> *«Uno es la omisión de autenticación, donde la funcionalidad se expuso de forma involuntaria a clientes de red no autenticados, y el otro es el recorrido de directorio donde la entrada no confiable (es decir, los parámetros en las solicitudes de red), no se desinfecta correctamente, permitiendo un acceso sin restricciones al sistema de archivos completo del servidor maestro».*

Los investigadores advirtieron que los defectos podrían explotarse en la naturaleza inminentemente. SaltStack también insta a los usuarios a seguir las mejores prácticas para proteger el entorno de Salt.

Vulnerabilidades en el protocolo ZeroMQ

Salt es un potente motor de automatización y ejecución remota basado en Python, que está diseñado para permitir a los usuarios emitir comandos a distintas máquinas directamente.

Creado como una utilidad para monitorear y actualizar el estado de los servidores, Salt emplea una arquitectura maestro-esclavo que automatiza el proceso de enviar actualizaciones de configuración y software desde un repositorio central usando un nodo

«maestro» que implementa los cambios en un grupo de «minions» (por ejemplo, servidores) en masa.

La comunicación entre un maestro y un súbdito se produce por medio del bus de mensajes ZeroMQ. Además, el maestro usa dos canales ZeroMQ, un «servidor de solicitud» al cual los minions informan los resultados de la ejecución, y un «servidor de publicación».

Según los investigadores de F-Secure, ambos defectos residen en el protocolo ZeroMQ de la herramienta.

> *«Las vulnerabilidades descritas en el aviso permiten a un atacante poder conectarse al puerto del «servidor de solicitudes», omitir todos los controles de autenticación y autorización y publicar mensajes de control arbitrarios, leer y escribir archivos en cualquier parte del sistema de archivos del servidor maestro y robar la clave secreta con la que el master se autentica como root»,* dijeron los investigadores.
>
> *«El impacto es la ejecución completa de comandos remotos como root tanto en el maestro como en todos los secuaces que se conectan a él»*.

Dicho de otro modo, un atacante puede explotar las vulnerabilidades para llamar a los comandos administrativos en el servidor maestro, así como los mensajes en cola directamente en el servidor de publicación maestro.

Además, una vulnerabilidad transversal del directorio identificada en el módulo de rueda, que tiene funciones para leer y escribir archivos en ubicaciones específicas, puede permitir la lectura de archivos fuera del directorio previsto debido a una falla en la desinfección adecuada de las rutas de los archivos.

Los investigadores de F-Secure dijeron que un escaneo inicial reveló más de 6000 instancias

vulnerables de Salt expuestas a Internet público.

La detección de posibles ataques contra maestros susceptibles, por lo tanto, implica auditar mensajes publicados a minions para cualquier contenido malicioso. *«La explotación de las vulnerabilidades de autenticación dará como resultado que las cadenas ASCII _prep_auth_info o _send_pub aparezcan en los datos enviados al puerto del servidor de solicitudes (predeterminado 4506)»*, dijeron los investigadores.

> *«Agregar controles de seguridad de red que restrinjan el acceso al maestro de Salt (los puertos 4505 y 4506 son los predeterminados) a los minios conocidos, o al menos bloquear el Internet más amplio, también sería prudente ya que los controles de autenticación y autorización proporcionados por Salt no son robustos actualmente para estar expuestos a redes hostiles»,* agregaron.