A pocos días de haber informado sobre dos vulnerabilidades críticas en el marco de configuración de SaltStack, una campaña de pirateo comenzó a explotar las vulnerabilidades para violar los servidores de LineageOS, Ghost y DigiCert.

Identificadas como CVE-2020-11651 y CVE-2020-11652, las vulnerabilidades reveladas podrían permitir que un adversario ejecute código arbitrario en servidores remotos implementados en centros de datos y entornos de nube. SaltStack solucionó los problemas en un comunicado publicado el 29 de abril.

> *«Esperamos que cualquier pirata informático competente pueda crear exploits 100% confiables para estos problemas en menos de 24 horas»,* advirtieron los investigadores de F-Secure.

LineageOS, fabricante de un sistema operativo de código abierto basado en Android, dijo que detectó la intrusión el 2 de mayo alrededor de las 8 pm, hora del Pacífico.

> *«Alrededor de las 8 pm PST del 2 de mayo de 2020, un atacante utilizó un CVE en nuestro maestro SaltStack para obtener acceso a nuestra infraestructura»*, dijo la compañía en su informe de incidentes.

Ghost, una plataforma de blogs basada en Node.js, también fue víctima de la misma falla. En su página web de estado, los desarrolladores afirmaron que *«alrededor de la 1:30 am UTC del 3 de mayo de 2020, un atacante usó un CVE en el maestro SaltStack para obtener acceso a nuestra infraestructura»,* además de instalar un minero de criptomonedas.

«El intento de minería aumentó las CPU y rápidamente sobrecargó la mayoría de los sistemas», agregó Ghost.

Ghost, sin embargo, confirmó que no había evidencia de que el incidente resultó en un

compromiso de los datos del cliente, las contraseñas y la información financiera.

Tanto LineageOS como Ghost restauraron los servicios luego de desconectar los servidores para parchear los sistemas y protegerlos detrás de un nuevo firewall.

En un desarrollo separado, la vulnerabilidad de Salt también se utilizó para piratear la autoridad de certificación DigiCert.

«Descubrimos hoy que la clave de CT Log 2 utilizada para firmar SCT (marcas de tiempo de certificado firmadas), se vio comprometida anoche a las 7 am por la vulnerabilidad de Salt», dijo el vicepresidente de producto de DigiCert, Jeremy Rowley, en una publicación de Google Groups el domingo.

> *«Aunque no creemos que la clave se haya utilizado para firmar STC (el atacante no parece darse cuenta de que obtuvieron acceso a las claves y estaban ejecutando otros servicios en la infraestructura), cualquier SCT proporcionada desde ese registro luego de las 7 pm MST ayer son sospechosos. El registro debe extraerse de la lista de registros de confianza».*