El fabricante de cajeros automáticos de Bitcoin, General Bytes, confirmó que fue víctima de un ataque cibernético que explotó una vulnerabilidad previamente desconocida en su software para robar criptomonedas a los usuarios.

> *«El atacante pudo crear un usuario administrador de forma remota por medio de la interfaz administrativa de CAS a través de una llamada URL en la página que se usa para la instalación predeterminada en el servidor y la creación del primer usuario administrador. Esta vulnerabilidad ha estado presente en el software CAS desde la versión 2020-12-08»,* dijo la compañía en un aviso la semana pasada.

CAS es la abreviatura de Crypto Application Server, un produco autohospedado de General Bytes que permite a las compañías administrar máquinas Bitcoin ATM dede una ubicación central a través de un navegador web en una computadora de escritorio o un dispositivo móvil.

La vulnerabilidad de día cero, que se refería a un error en la interfaz de administración de CAS, se mitigó en dos versiones de parches del servidor; 20220531.38 y 20220725.22.

General Bytes dijo que el atacante sin nombre identificó la ejecución de servidores CAS en los puertos 7777 o 443 al escanear el espacio de direcciones IP de alojamiento en la nube de DigitalOcean, y después abusó de la vulnerabilidad para agregar un nuevo usuario administrador predeterminado llamado «gb» al CAS.

> *«El atacante modificó la configuración criptográfica de las máquinas bidireccionales con la configuración de la billetera y la configuración de 'dirección de pago no válida'. Los cajeros automáticos bidireccionales comenzaron a enviar monedas a la billetera del atacante cuando los clientes enviaban monedas al cajero automático»,* agregó la compañía.

El objetivo del ataque era modificar la configuración de tal forma que todos los fondos se transfirieran a una dirección de billetera digital bajo el control del adversario.

La compañía también enfatizó que había realizado *«múltiples auditorías de seguridad»* desde 2020 y que esta vulnerabilidad nuca se identificó.