Avviso tecnico: vulnerabilità di sicurezza scoperta nelle stampanti CL4/6NX Plus

30 sep 2024

Sommario

È stato scoperto che alcune stampanti SATO presentano vulnerabilità relative ad autorizzazioni errate/non corrette (CWE-863, CWE-287) e path traversal (CWE-22) che potrebbero portare a modifiche non autorizzate delle impostazioni e manomissioni dei file, con un impatto potenziale sul funzionamento delle stampanti.

Non sono noti casi di sfruttamento di queste vulnerabilità e gli utenti non corrono alcun rischio di manomissione dei dati o esposizione delle informazioni purché adottino misure per proteggere i propri sistemi da accessi non autorizzati.

Tuttavia, consigliamo di seguire la procedura riportata di seguito per una maggiore sicurezza.

Stampanti interessate

- CL4/6NX Plus
- CL4/6NX-J Plus (solo Giappone)

Soluzione

Un aggiornamento del firmware della stampante che va a correggere queste vulnerabilità è in fase di sviluppo. Per informazioni sull'aggiornamento, contatta il tuo ufficio SATO di riferimento o il rivenditore/distributore presso cui hai acquistato la stampante. Se hai bisogno di parlare con noi, clicca qui.

Work-around

Le vulnerabilità possono essere aggirate abilitando il firewall della stampante e disabilitando la funzione WebConfig (si tratta della funzione che permette di gestire le impostazioni della stampante via browser) solo in caso non si riesca ad installare l'aggiornamento del firmware per determinati motivi tecnici.

Si prega di notare che la soluzione sopracitata è temporanea e che idealmente si dovrebbe rimediare alle vulnerabilità tramite la patch di sicurezza non appena la situazione lo consentirà.

I passi elencati di seguito illustrano il metodo sopracitato. Per maggiori informazioni, fare riferimento alla sezione “Various Settings of the Product” del manuale utente che si trova a questo link.

- Abilitare il firewall:
  Andare al menù impostazioni stampante> Network> Advanced> Firewall> Enable.
- Disabilitare il WebConfig:
  Andare al menù impostazioni stampante > Network> Advanced> Firewall> Allow Services and Ports> WebConfig> Disable.

Per domande o dubbi, scrivici cliccando qui.