Policy för ansvarsfull information om utsatthet

Vi tar säkerheten för våra system på allvar och vi välkomnar feedback från säkerhetsundersökare för att förbättra säkerheten för våra produkter och tjänster.

Vi kräver att alla våra undersökare tar hänsyn till respekten för lagen. Sårbarhetsskanning kunde inte fungera som en förevändning för att attackera ett system eller något annat mål. Flera åtgärder måste undvikas. Till exempel:

- Använda socialteknik
- Äventyra systemet och upprätthålla åtkomst till det
- Ändra åtkomst till data genom att utnyttja sårbarheten
- Använda skadlig kod
- Att använda sårbarheten på något sätt utöver att bevisa dess existens. För att visa att sårbarheten finns kan reportern använda icke-påträngande metoder. Till exempel lista en systemkatalog
- Använd brute force för att få tillgång till system
- Dela sårbarhet med tredje part
- Utföra DoS- eller DDoS-attacker

Spara information om eventuella sårbarheter som du har upptäckt konfidentiellt mellan dig och Salto Systems tills vi löser problemet.

Skicka ett mejl till securityalert@saltosystems.com om du har identifierat några problem som kan påverka säkerheten för våra produkter eller tjänster.

Vi bjuder in etiska hackare att upptäcka sårbarheter genom vårt Bug Bounty-program på Intigriti.

Vi strävar efter att bekräfta mottagandet av din sårbarhetsrapport inom 7 arbetsdagar och att slutföra triageprocessen inom 14 arbetsdagar. Under hela processen kommer vi att hålla dig uppdaterad om våra framsteg och slutförandet av eventuella saneringsinsatser genom vårt Bug Bounty-program.

Om ytterligare information behövs kan vi kontakta dig för förtydligande. Åtgärdandet av rapporterade sårbarheter prioriteras baserat på faktorer som påverkan, svårighetsgrad och utnyttjande av komplexitet. Med tanke på dessa överväganden kan vissa rapporter kräva ytterligare tid för triage eller lösning. Du är välkommen att checka in på statusen, men vi ber dig att göra det inte mer än en gång var 14:e dag för att låta våra team fokusera på avhjälpande aktiviteter.

För vissa av våra produkter bjuder vi dessutom in etiska hackare att hitta sårbarheter genom vårt Bug Bounty-program på Intigriti.

Bli belönad för att göra oss starkare! Registrera dig här.

Ansvarsfriskrivning:

Detta är en nedladdningsbar version av webbplatsens innehåll som vi tillhandahåller för informationssyften, för att underlätta konsultation och ifyllande. Salto åtar sig dock inget ansvar för eventuella fel eller tryckfel som den nedladdningsbara versionen kan innehålla.

En del av innehållet på denna webbplats kan ha genererats av eller skapats med hjälp av AI-verktyg. Webbplatsen kan även erbjuda automatiska eller manuella översättningar endast i informationssyfte, vilka kan innehålla fel eller brister. Salto garanterar inte korrektheten, kvaliteten eller tillförlitligheten hos sådant innehåll eller sådana översättningar, inklusive sådana som genererats av AI.

Användaren ansvarar för att verifiera den information som finns i detta dokument och ska, i händelse av tvivel, hänvisa till den engelska originalversionen, som gäller vid eventuella avvikelser. Andra språkversioner tillhandahålls enbart för informationssyften.

Fastän Salto gör rimliga ansträngningar för att granska innehållet i sina nedladdningsbara dokument, kan de innehålla fel eller utelämnanden. Salto åtar sig inget ansvar för eventuella skador eller beslut som grundar sig på användningen, tolkningen eller de beslut som användaren fattar baserat på informationen i detta dokument, vilket används på användarens eget ansvar.

För mer detaljerad information om användningen av artificiell intelligens, översättningar och gällande ansvarsbegränsningar, se ”Användarvillkor för vår webbplats”.

Salto förbehåller sig rätten att ändra detta innehåll från tid till annan. Vänligen kontrollera i det juridiska avsnittet på vår webbplats för att hitta den senaste versionen av de juridiska dokumenten och deras uppdateringar.