Politik for offentliggørelse af sårbarheder

Vi tager sikkerheden af vores systemer alvorligt, og vi værdsætter feedback fra sikkerhedsforskere for at forbedre sikkerheden af vores produkter og tjenester.

Vi kræver, at alle forskere tager hensyn til og respekterer lovgivningen. Sårbarhedsscanning vil ikke kunne fungere som et påskud til at angribe et system eller et andet mål. Flere handlinger skal undgås. For eksempel:

- Brug af social manipulation
- Kompromittering af systemet og vedvarende opretholdelse af adgang til det
- Ændring af de data, der tilgås ved at udnytte sårbarheden
- Brug af malware
- Brug af sårbarheden på nogen måde ud over at bevise dens eksistens. For at påvise, at sårbarheden eksisterer, kan indberetteren måske bruge ikke-indgribende metoder. F.eks. en liste over en systemmappe
- Brug af vold til at få adgang til systemer
- Deling af sårbarhed med tredjeparter
- Udførelse af DoS- eller DDoS-angreb

Hold oplysninger om eventuelle sårbarheder, du har opdaget, fortrolige mellem dig selv og Salto Systems, indtil vi løser problemet.

Send en e-mail til securityalert@saltosystems.com, hvis du har identificeret et problem, der potentielt kan påvirke sikkerheden af vores produkter eller tjenester.

Vi inviterer etiske hackere til at opdage sårbarheder gennem vores Bug Bounty Program på Intigriti.

Vi bestræber os på at bekræfte modtagelsen af din rapport om sårbarheder inden for 7 hverdage og gennemføre den indledende vurdering (triage) senest 14 hverdage efter. I hele forløbet holder vi dig løbende orienteret om status og eventuelle tiltag via vores bug bounty-program.

Hvis vi har brug for yderligere oplysninger, kontakter vi dig for en afklaring. Rapporterne prioriteres ud fra faktorer som påvirkning, alvorlighed og hvor komplekse de er at udnytte. Nogle sager kan derfor kræve længere tid til vurdering eller løsning. Du er altid velkommen til at følge op på status, men vi beder dig om at gøre det højst én gang hver 14. dag, så vores teams kan fokusere på at håndtere sårbarhederne.

For nogle af vores produkter inviterer vi desuden etiske hackere til at finde sårbarheder gennem vores Bug Bounty Program på Intigriti.

Bliv belønnet for at hjælpe os med at blive endnu sikrere – Tilmeld dig her.

Disclaimer:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, SALTO assumes no responsibility for any errors or typos that the downloadable version may contain.

As SALTO reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.