

# Vastuullinen haavoittuvuuksien julkistamiskäytäntö

Suhtaudumme järjestelmiemme turvallisuuteen vakavasti ja otamme mielellämme vastaan palautetta tietoturvatutkijoilta, jotta voimme parantaa tuotteidemme ja palveluidemme turvallisuutta.

Edellytämme, että kaikki tutkijat ottavat huomioon tarpeen kunnioittaa lakia. Haavoittuvuuksien skannaus ei voi toimia tekosyynä järjestelmään tai muuhun kohteeseen hyökkäämiselle. On useita toimia, joita on vältettävä.

Esimerkiksi seuraavia:

- › Käyttäjän manipulointi
- › Järjestelmän vaarantaminen ja järjestelmään pääsyn jatkuva ylläpitäminen
- › Haavoittuvuutta hyödyntämällä käytetyn tiedon muuttaminen
- › Haittaohjelmien käyttö
- › Haavoittuvuuden käyttäminen muulla tavoin kuin sen olemassaolon todistamiseksi. Haavoittuvuuden olemassaolon osoittamiseksi raportoija voi käyttää ei-tunkeutuvia menetelmiä, esimerkiksi järjestelmähakemiston listaamista.
- › Pääsy järjestelmiin raa'an voimankäytön avulla
- › Haavoittuvuuden jakaminen kolmansien osapuolten kanssa
- › Palvelunesto- tai hajautettujen palvelunestohyökkäysten suorittaminen

Pidä havaitsemiasi haavoittuvuuksia koskevat tiedot luottamuksellisina sinun ja Salto Systemsin välillä, kunnes ongelma on ratkaistu.

Lähetä sähköpostia osoitteeseen [securityalert@saltosystems.com](mailto:securityalert@saltosystems.com), jos olet havainnut jonkin ongelman, joka saattaa vaikuttaa tuotteidemme tai palveluidemme turvallisuuteen.

Reagoimme raporttisi vastaanottamiseen ripeästi.

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.