

Beleid inzake verantwoordelijke openbaarmaking van kwetsbaarheden

We nemen de beveiliging van onze systemen serieus en verwelkomen feedback van beveiligingsonderzoekers om de beveiliging van onze producten en diensten te verbeteren.

Wij eisen dat alle onderzoekers rekening houden met het respect voor de wet. Kwetsbaarheidsscanning mag niet dienen als een excuus voor het aanvallen van een systeem of enig ander doelwit. Verschillende acties moeten vermeden worden. Bijvoorbeeld:

- › Het gebruiken van social engineering.
- › Het systeem compromitteren en er voortdurend toegang toe behouden
- › De gegevens wijzigen waartoe toegang is verkregen door misbruik te maken van de kwetsbaarheid
- › Malware gebruiken
- › De kwetsbaarheid op een andere manier gebruiken dan alleen het bestaan ervan bewijzen. Om aan te tonen dat de kwetsbaarheid bestaat, kan de melder niet-intrusieve methoden gebruiken. Bijvoorbeeld het vermelden van een systeemmap
- › Brute kracht gebruiken om toegang tot systemen te krijgen
- › Kwetsbaarheid delen met derden
- › DoS- of DDoS-aanvallen uitvoeren

Houd informatie over eventuele kwetsbaarheden die u hebt ontdekt vertrouwelijk tussen uzelf en Salto KS | Salto Systems totdat we het probleem hebben opgelost.

Stuur een e-mail naar [securityalert@salto**systems.com**](mailto:securityalert@saltosystems.com) als u een probleem hebt ontdekt dat mogelijk van invloed kan zijn op de beveiliging van onze producten of diensten.

We zullen uw melding onmiddellijk bevestigen.

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.