

Poniższa lista ostrzeżeń dotyczących bezpieczeństwa użytkowania produktu oparta jest o wymagania Rozporządzenia (UE) 2023/988 (GPSR). Naszym celem jest ochrona użytkowników przed potencjalnymi zagrożeniami wynikającymi z nieodpowiedniego użytkowania. Informacje przedstawione są w prosty sposób by były zrozumiałe i przejrzyste dla wszystkich użytkowników, w tym również dla osób starszych oraz osób z ograniczeniami ruchowymi.

Instrukcja bezpieczeństwa użytkowania produktu SG3452X - switch gigabitowy 48-port + 4 SFP+

1. Ogólne zasady bezpieczeństwa

- Przed obsługą urządzenia należy zapoznać się z instrukcją obsługi produktu dostarczoną przez producenta i informacjami dotyczącymi bezpieczeństwa w niej zawartymi.
- Używaj produkt zgodnie z jego przeznaczeniem określonym w instrukcji obsługi.
- To urządzenie może być używane wyłącznie przez osoby o wystarczającej sprawności fizycznej, sensorycznej i intelektualnej oraz posiadającej odpowiednią wiedzę i doświadczenie. Inne osoby mogą korzystać z urządzenia wyłącznie pod nadzorem osób odpowiedzialnych za ich bezpieczeństwo.
- Trzymaj ten produkt z dala od dzieci. Dzieci nie są jeszcze w stanie ocenić istniejących zagrożeń.
- Przechowywać elementy opakowania (woreczki foliowe, elementy ze styropianu) poza zasięgiem dzieci i zwierząt.

2. Bezpieczeństwo montażu i instalacji

- Switche SFP należy montować w stabilnych szafach lub stojakach RACK, używając dołączonych uchwytów montażowych.
- Przed instalacją upewnij się, że miejsce montażu jest suche, wolne od kurzu i zapewnia odpowiednią wentylację, aby uniknąć przegrzania urządzenia.
- Nie blokuj otworów wentylacyjnych na obudowie urządzenia, aby zapewnić prawidłowe chłodzenie.
- Podczas montażu unikaj uszkodzenia portów SFP i kabli światłowodowych, stosując odpowiednie narzędzia i delikatność.

3. Bezpieczeństwo elektryczne i zasilania

- Podłączaj urządzenie wyłącznie do gniazd zasilających z odpowiednim napięciem (100-240V AC) i zabezpieczeniem przeciwprzepięciowym.
- W przypadku urządzeń z redundantnym zasilaniem stosuj wyłącznie zasilacze i kable dostarczone lub zalecane przez producenta.
- Nie uszkodzaj przewodów zasilających i nie ciągnij za nie podczas odłączania urządzenia.
- W przypadku uszkodzenia zasilania lub podejrzenia awarii natychmiast odłącz urządzenie i skontaktuj się z serwisem.

4. Bezpieczeństwo użytkowania i eksploatacji

- Nie używaj uszkodzonych urządzeń ani kabli światłowodowych, aby uniknąć ryzyka uszkodzenia sprzętu lub przerw w transmisji danych.
- Nie demontuj ani nie modyfikuj urządzenia; wszelkie naprawy powinny być wykonywane przez wykwalifikowany personel.

- Podczas podłączania i odłączania modułów SFP zachowaj ostrożność, aby nie uszkodzić portów ani modułów.
- Nie patrz bezpośrednio w światło emitowane przez moduły SFP, gdyż może to uszkodzić wzrok.
- Unikaj pracy z urządzeniem pod wpływem alkoholu lub środków odurzających.
- Zachowaj czystość portów SFP i kabli światłowodowych, aby zapewnić stabilną transmisję sygnału.

5. Bezpieczeństwo sieci i danych

- Konfiguruj urządzenie zgodnie z zaleceniami producenta, stosując odpowiednie zabezpieczenia sieciowe, takie jak VLAN, ACL i QoS.
- Regularnie aktualizuj oprogramowanie urządzenia, aby zapewnić ochronę przed znanymi zagrożeniami.
- Monitoruj stan urządzenia i sygnalizację LED, aby szybko wykrywać i reagować na ewentualne problemy.

6. Bezpieczeństwo konserwacji

- Przed przystąpieniem do czyszczenia lub serwisowania urządzenia odłącz je od zasilania.
- Do czyszczenia obudowy używaj miękkiej, suchej szmatki; nie stosuj środków chemicznych ani rozpuszczalników.
- Nie otwieraj obudowy urządzenia, aby uniknąć ryzyka porażenia prądem lub uszkodzenia komponentów.

7. Zagrożenia cyberbezpieczeństwa

- Urządzenie musi być zabezpieczone przed nieautoryzowanym dostępem. Używaj tylko silnych haseł.
- Regularna zmiana hasła jest podstawowym elementem odpowiedniego zabezpieczenia systemu.
- Należy stosować ograniczenia uprawnień użytkowników urządzenia. Każdy użytkownik powinien mieć tylko niezbędne uprawnienia.
- Jeżeli to możliwe wykonuj segmentację sieci za pośrednictwem VLAN. Odpowiednio podzielona sieć pozwala na odseparowanie ruchu pomiędzy poszczególnymi grupami urządzeń.
- Unikaj bezpośredniego wystawiania urządzenia do sieci publicznej poprzez przekierowanie portów. Do dostępu zdalnego korzystaj z funkcji chmurowych, jeżeli urządzenie je posiada lub z połączeń VPN.
- Jeżeli urządzenie posiada panel WEB, korzystaj z szyfrowanych połączeń HTTPS.
- Należy regularnie przeprowadzać aktualizację oprogramowania urządzenia aby zapewnić ochronę przed nowymi zagrożeniami.
- Należy zapewnić wszystkie możliwe środki ochrony sieci i danych osobowych.
- Wyłącz funkcje sieciowe i protokoły jak UPnP, jeżeli nie są potrzebne we wdrażanym systemie.
- Regularnie wykonuj audyty bezpieczeństwa, co pewien czas należy przeprowadzać testy bezpieczeństwa i aktualizować polityki ochrony.

8. Prawidłowe usuwanie zużytego urządzenia

- Produkt należy utylizować zgodnie z miejscowymi przepisami dotyczącymi gospodarki odpadami elektronicznymi i niebezpiecznymi.

9. Znaczenie stosowania się do ostrzeżeń

- Zastosowanie się do przedstawionych tu ostrzeżeń minimalizuje ryzyko uszkodzeń ciała, awarii urządzenia oraz strat materialnych wynikających z nieumiejętnego obchodzenia się produktem.

Na każdym etapie użytkowania urządzenia należy przestrzegać zasad i informacji bezpieczeństwa zawartych w instrukcji obsługi produktu dostarczonej przez producenta. Zachowaj instrukcję obsługi abyś mógł się w każdej chwili do niej odnieść. Urządzenie należy przekazywać osobom trzecim wyłącznie wraz z instrukcją użytkowania.