# CVE-2020-12812

## Opis podatności

Luka w zabezpieczeniach nieprawidłowego uwierzytelniania w SSL VPN w FortiOS 6.4.0, 6.2.0 do 6.2.3, 6.0.9 i starszych wersjach może spowodować, że użytkownik będzie mógł pomyślnie zalogować się bez pytania o drugi czynnik uwierzytelnienia (FortiToken), jeśli zmienili wielkość liter w swojej nazwie użytkownika.

**Base Score:**  9.8 CRITICAL

**Vector:**  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## Algorytm działania

Luka w nieprawidłowym uwierzytelnianiu w SSL VPN w FortiOS może spowodować, że użytkownik będzie mógł pomyślnie zalogować się bez pytania o drugi czynnik uwierzytelnienia (FortiToken), jeśli zmieni wielkość liter w swojej nazwie użytkownika.

Dzieje się tak, gdy w ustawieniu „użytkownik lokalny” jest włączone uwierzytelnianie dwuskładnikowe, a typ uwierzytelniania użytkownika jest ustawiony na metodę uwierzytelniania zdalnego (np.: ldap).

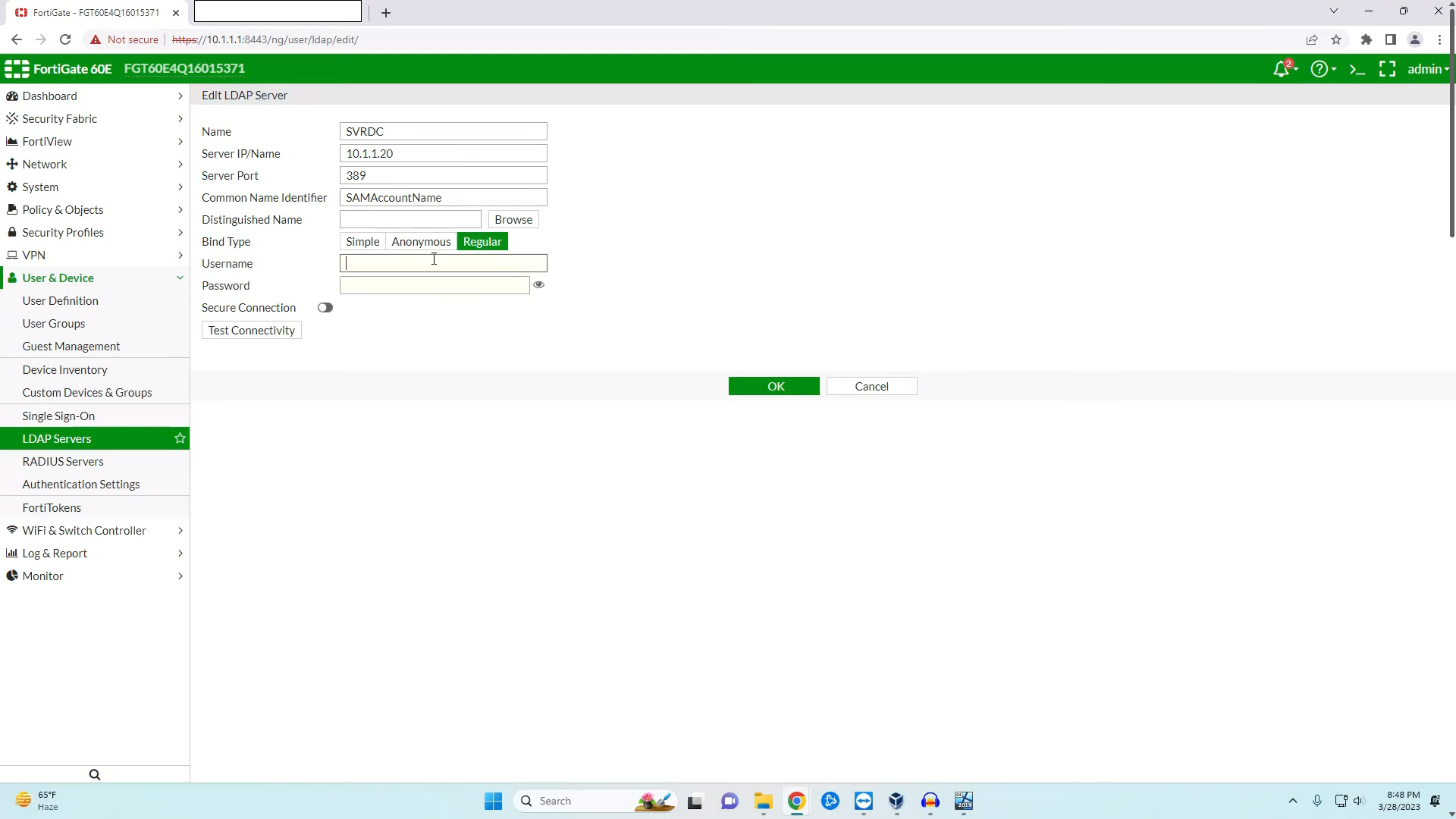
Problem występuje z powodu niespójnego dopasowywania wielkości liter w uwierzytelnianiu lokalnym i zdalnym.

## Realizacja

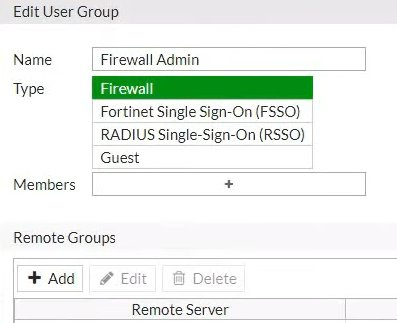
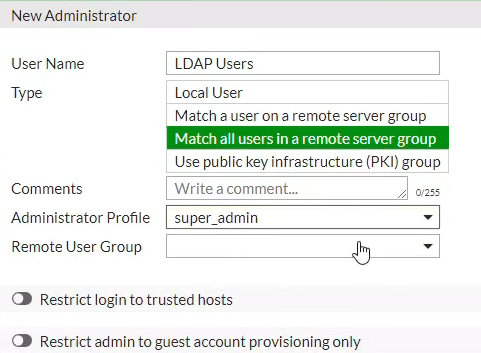
Niestaty, nie udało się zainstalować narzędzie, aby przetestować atak, ponieważ nie ma możliwości zciągnięcia odpowiedniej wersji.

Jakby to działało na FortiGate:

Konfigurowany jest serwer LDAP i użytkownik localny o tej samej nazwie, która jest używana dla konta LDAP oraz przydzielić użytkownika do właściwej grupy. Przykładowo:



Rysunek 1. Konfiguracja serweru LDAP w FortiGate



Rysunek 2. Przydzielienie grupy użytkowników

Dodawani użytkownicy muszą mieć przypisane FortiTokeny. Następnie dodajemy grupę do zasad ruchu przychodzącego SSL VPN, korzystujemy z opcji „Remote access LDAP and Token”:

A screenshot of a computer

Description automatically generated

Rysunek 3. Dodanie zasad ruchu

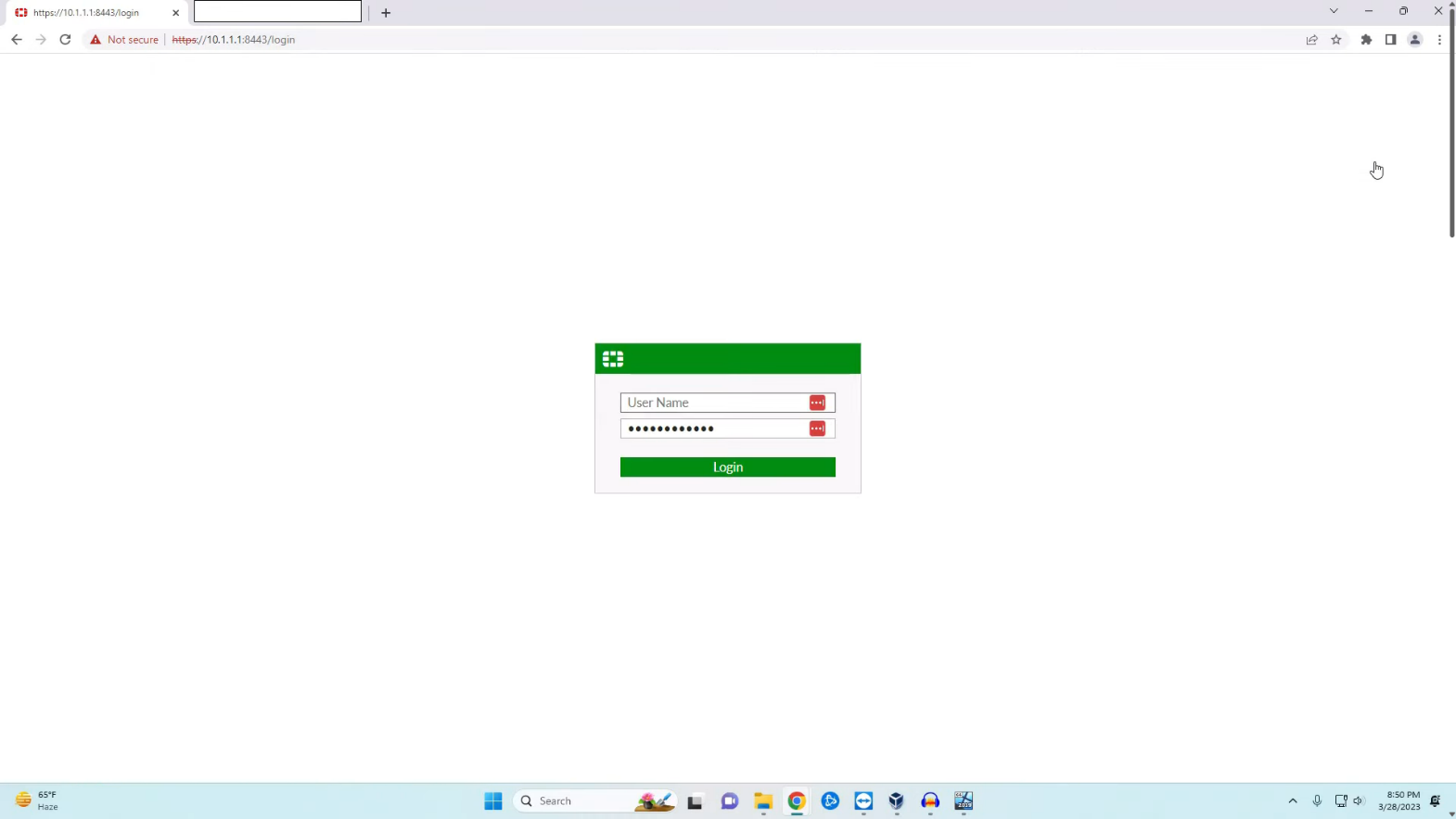
Do reguł uwierzytelniania dodajemy stworzoną grupę lokalną:

A screenshot of a computer

Description automatically generated

Rysunek 4. Dodanie reguły uwierzytelnienia

Na tym etapie można podjąć próbę logowania. Strona logowania:



Rysunek 5. Strona logowania

Wpisujemy nazwę użytkownika, zmieniając wielkość liter i musimy poprawnie zalogować się bez pytania o FortiToken.

## Podsumowanie

Trudno jest skorzystać z tej podatności. Wersję systemu w którym można było z tego skorzystać już niedostępne do zainstalowania. Ponadto, atakujący musi wiedzieć nazwę użytkownika i prawidłowe hasło aby przeprowadzić atak. Musi też mieć możliwość połączenia z systemem webowym FortiOS albo CLI, tzn. być w jednej sieci z systemem ofiary. System ofiary także musi być odpowiednio skonfigurowany.

Aby uniknąć problemu związanego z obejściem uwierzytelniania, administratorzy muszą ręcznie wyłączyć rozróżnianie wielkości liter w nazwie użytkownika. Zainstalowanie nowszej wersji jest zalecane.