Host	192.168.100.20
Port	5900/TCP
(QoD)	95%
CVSS	10.0

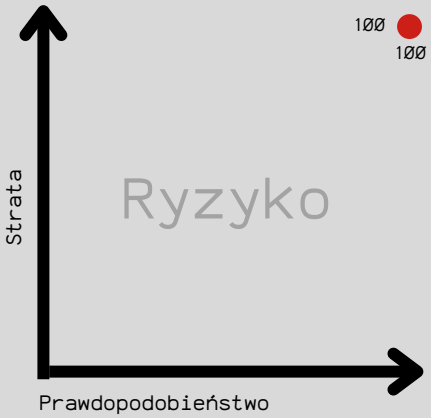
Opis podatności

Skaner OpenVas oraz Nessus wykrył możliwość zalogowania sie do maszyny za wykorzystaniem słabej jakości haseł. Niezabezpieczony zasób dopuszcza możliwość wielokrotnych prób logowania co stanowi wysokie ryzyko przeprowadzenia udanego ataku z wykorzystaniem słowników haseł, w celu uzyskania poświadczeń administratorskich

Próby logowania mogą być rejestrowane w logach VNC lub wykrywane przez systemy HIDS/NIDS, o ile są odpowiednio skonfigurowane. Brak ograniczeń po stronie aplikacji utrudnia automatyczną blokadę ataku.

Tego typu podatność może stanowić poważne naruszenie wymagań zgodności z ISO/IEC 27001, PCI-DSS lub RODO, ze względu na brak kontroli dostępu i narażenie danych użytkowników.

„Brak limitu prób logowania znacząco zwiększa ryzyko przejęcia konta użytkownika, zwłaszcza przy słabych hasłach”
— OWASP Authentication Cheat Sheet



Ryzyko

Scenariusze ataku

Atak słownikowy

Atak Brute-Force

Host	192.168.100.20
Port	5900/TCP
(QoD)	95%
CVSS	10

Mapa zagrożeń

Pełna kontrola nad systemem - Atakujący zyskuje dostęp do pulpitu jak lokalny użytkownik, co pozwala mu m.in. kraść lub niszczyć dane, zmieniać ustawienia, instalować/zdejmować oprogramowanie oraz przejmować dalszą kontrolę nad infrastrukturą IT.

Dostęp do systemów krytycznych - W środowiskach przemysłowych, takich jak systemy SCADA czy HMI, przejęcie VNC może umożliwić sterowanie sprzętem produkcyjnym, powodując realne straty, awarie lub zagrożenie dla zdrowia i życia.

Kradzież danych i przechwytywanie sesji - W klasycznym VNC brak domyślnego szyfrowania oznacza przesyłanie wszystkiego (w tym haseł, obrazów ekranu, danych poufnych) w postaci jawnej, co pozwala przechwycić je każdemu na trasie transmisji („podsłuch sesji").

Zdalne wykonanie kodu (RCE) - Historyczne i bieżące podatności (np. CVE-2022-23854 w TigerVNC) pozwalają na uruchamianie dowolnego kodu na komputerze ofiary bez jej wiedzy.

Rozprzestrzenianie się ataku wewnątrz organizacji - Po uzyskaniu przyczółka, atakujący może skanować i infekować inne maszyny w tej samej sieci, eskalując uprawnienia lub przygotowując ataki na kolejne cele.

Ominięcie zabezpieczeń - Atakujący może wyłączyć programy antywirusowe, firewalle czy inne zabezpieczenia, zacierać ślady i zmieniać logi systemowe.

Wykorzystanie komputera do dalszych ataków - Przejęty system może posłużyć do ataków na inne organizacje (np. przechwytywanie tuneli VPN lub przeprowadzanie ataków brute force na kolejne usługi).

Podszywanie się i wyłudzenia - Możliwe jest wysyłanie wiadomości e-mail, wyłudzanie dodatkowych danych lub prowadzenie dalszych ataków socjotechnicznych jako "właściciel" przejętego komputera.

Host	192.168.100.20
Port	5900/TCP
(QoD)	95%
CVSS	10

Wektory ataku

1. Atak Słownikowy na hasło VNC

Próby zgadywania hasła przy użyciu narzędzi automatyzujących logowanie (np. Hydra, Medusa, Ncrack).
Wykorzystanie słowników typowych, słabych lub domyślnych haseł.
Celu ataku: uzyskanie autoryzowanego dostępu do sesji VNC przy użyciu programu Hydra

Ryzyko:
Poufność (Confidentiality)
● Zagrożona
Jeśli atak się powiedzie, napastnik uzyskuje pełen dostęp do sesji pulpitu - widzi pliki, dane, otwarte dokumenty. Może odczytać wrażliwe informacje.
Integralność (Integrity)
● Zagrożona
Po uzyskaniu dostępu napastnik może modyfikować pliki, instalować złośliwe oprogramowanie lub manipulować konfiguracją systemu.
Dostępność (Availability)
● Zagrożona
Intensywne próby logowania mogą doprowadzić do tymczasowego zablokowania konta lub usługi VNC (np. przez mechanizmy anty-brute-force, limit logowań). Może to również przeciążyć usługę.

Uwagi do raportu:
Nawet nieudany brute force może zakłócić dostępność usługi.
Użycie słabych/domyślnych haseł znacząco zwiększa prawdopodobieństwo sukcesu ataku.
Jeśli środowisko testowe nie ma limitu prób logowania — jest to poważne niedopatrzenie konfiguracyjne.
Brak mechanizmów typu CAPTCHA, blokady IP, lub 2FA to również czynnik ryzyka.

Host	192.168.100.20
Port	5900/TCP
(QoD)	95%
CVSS	10

3d. Narzędzia i zasoby organizacyjne

OpenVAS

Niniejszy skrypt podejmuje próbę uwierzytelnienia w serwerze VNC, wykorzystując hasła zdefiniowane w ustawieniach preferencyjnych. Dodatkowo testuje, czy dostęp do serwera nie jest możliwy bez potrzeby podawania hasła lub przy braku jakiejkolwiek autoryzacji i raportuje taki przypadek.

Nessus

.

Narzędzie Nessus było w stanie uzyskać dostęp przy użyciu domyślnego hasła „password”. Oznacza to, że potencjalny, nieautoryzowany atakujący mógłby przejąć kontrolę nad systemem

nmap

Potwierdza obecność vnc, w wersji 3.3

Hydra

Wykonanie ataku typu brute-force na usługę VNC

3e. Ograniczenia testów & Zakres wykluczeń

BRAK

Host	192.168.100.20
Port	5900/TCP
(QoD)	95%
CVSS	10

Załączniki

Załącznik 1 - 192.168.100.20-openvas.pdf

2.1.13 High 5900/tcp

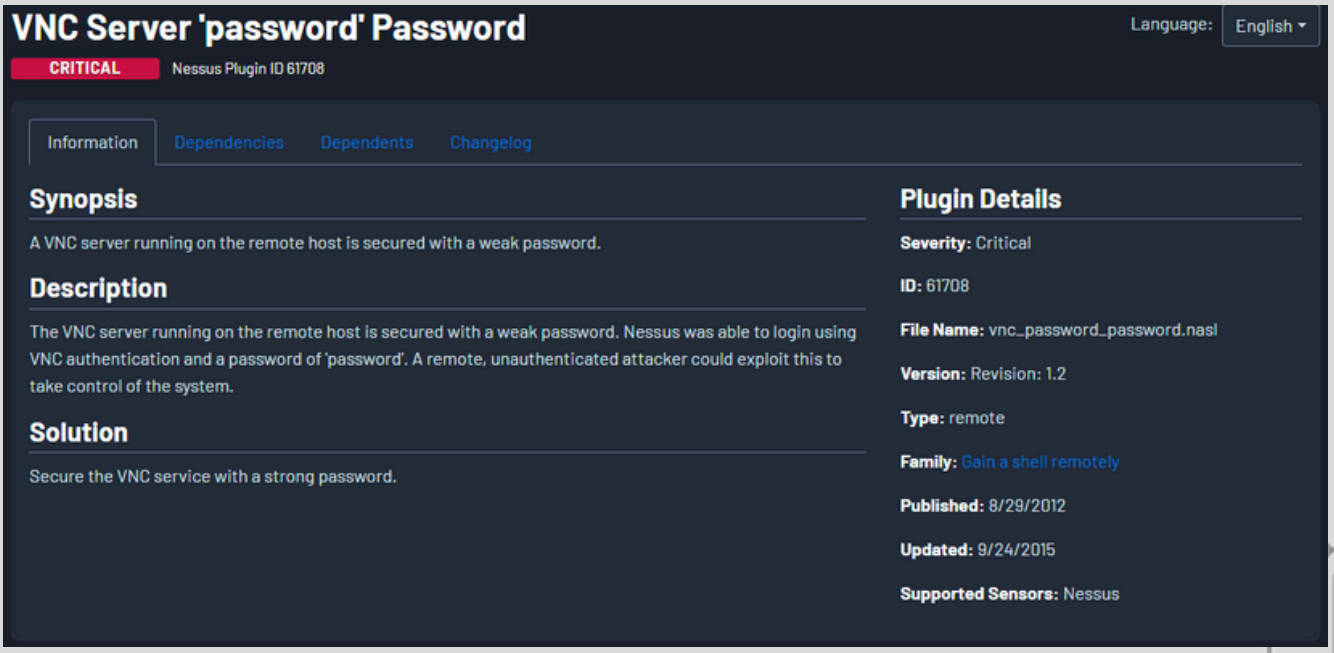
High (CVSS: 9.0)

NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Details: VNC Brute Force Login
OID:1.3.6.1.4.1.25623.1.0.106056
Version used: 2021-07-23T07:56:26Z

Załącznik 2 - 192.168.100.20-nessus.pdf



Załącznik 3 - 192.168.100.20-vulnTCP.nmap

```
5900/tcp  open  vnc          VNC (protocol 3.3)
```