

ESPLORAZIONE DEI CVE TRAMITE ChatGPT

OBIETTIVO: L'OBIETTIVO DI QUESTO ESERCIZIO È IMPARARE A UTILIZZARE ChatGPT PER RACCOGLIERE INFORMAZIONI SUI CVE (COMMON VULNERABILITIES AND EXPOSURES). QUESTO ESERCIZIO VI GUIDERÀ ATTRAVERSO IL PROCESSO DI FORMULAZIONE DI UNA RICHIESTA (PROMPT) EFFICACE PER OTTENERE UNA LISTA DI CVE E INFORMAZIONI DETTAGLIATE SU CIASCUNO DI ESSI.

IN QUESTO REPORT UTILizzeremo SEMPRE UN PROMPT SU ChatGPT CHE CI SPIEGHI QUALI SONO I CVE, IN QUESTO CASO DI WINDOWS 10; HO SCELTO DI RACCOGLIERE INFORMAZIONI SU QUESTO SISTEMA OPERATIVO, MA POTEVO SCEGLIERE ANCHE ALTRI SOFTWARE O SISTEMI OPERATIVI;

SIAMO ANDATI A SCRIVERE IL NOSTRO PROMPT SU L'AI E VEDIAMO LE SUE RISPOSTE SE SODDISFANO LE NOSTRE RICHIESTE: adesso elencami i principali CVE del sistema operativo windows 10. dopodichè descrivimi bene ognuno di essi dicendomi le vulnerabilità e cosa fare per contrastarle;

adesso elencami i principali CVE del sistema operativo windows 10.
dopodichè descrivimi bene ognuno di essi dicendomi le vulnerabilità e
cosa fare per contrastarle

Di seguito trovi un **elenco ragionato dei principali CVE che hanno colpito Windows 10**, scelti perché molto diffusi, critici o storicamente rilevanti, seguiti da una **descrizione dettagliata di ciascuno**, delle vulnerabilità sfruttate e delle contromisure efficaci.

⚠️ Nota importante

Windows 10 ha **centinaia di CVE** ogni anno. Qui trovi i **più importanti e studiati**, spesso citati in corsi di cybersecurity, certificazioni ed esami.

Principali CVE di Windows 10

1. CVE-2017-0144 – EternalBlue

Gravità: 🔴 Critica

Categoria: Remote Code Execution (RCE)

Descrizione

EternalBlue è una vulnerabilità nel **protocollo SMBv1** di Windows, scoperta dalla NSA e poi trapelata dal gruppo Shadow Brokers.



Per saperne di più su questa vulnerabilità:

+ | Fai una domanda



ChatGPT CI HA SUBITO SPECIFICATO CHE WINDOWS 10 HA CENTINAIA DI CVE E CHE QUINDI NON POTEVA SCRIVERE TUTTI, MA RIPORTA SOLO I PIÙ IMPORTANTI E DIFFUSI, COME CHIESTO DA NOI;

E COME POSSIAMO VEDERE ANCHE DAI SEGUENTI SCREEN, HA CITATO 7 CVE DI WINDOWS 10:

◆ Fai l'upgrade a Go ×

1. CVE-2017-0144 – EternalBlue

Gravità: ● Critica

Categoria: Remote Code Execution (RCE)

Descrizione

EternalBlue è una vulnerabilità nel **protocollo SMBv1** di Windows, scoperta dalla NSA e poi trapelata dal gruppo Shadow Brokers.

Permette a un attaccante remoto di:

- eseguire codice arbitrario
- **senza autenticazione**
- semplicemente inviando pacchetti malevoli SMB

Perché è pericolosa

- Non richiede interazione dell'utente
- Si diffonde automaticamente in rete
- È stata usata da **WannaCry** e **NotPetya**

Impatto

- Compromissione completa del sistema
- Propagazione worm-like

Contromisure

- ✓ Installare patch Microsoft (MS17-010)
- ✓ Disabilitare SMBv1
- ✓ Segmentazione di rete
- ✓ Firewall: bloccare porta TCP 445



+ | Fai una domanda



ChatGPT può commettere errori. Assicurati di verificare le informazioni importanti. Vedi [Preferenze sui cookie](#).

2. CVE-2020-1472 – ZeroLogon

Gravità:  Critica

Categoria: Privilege Escalation / Authentication Bypass

Descrizione

Vulnerabilità nel Netlogon Remote Protocol.

Consente a un attaccante di:

- azzerare la password del Domain Controller
- ottenere privilegi di amministratore di dominio
- con pochissimi tentativi

Perché è pericolosa

- Attacco rapidissimo
- Compromissione totale del dominio Active Directory

Impatto

- Controllo completo dell'infrastruttura Windows
- Movimento laterale illimitato

Contromisure

- ✓ Patch Microsoft (agosto 2020)
- ✓ Forzare modalità "Enforcement" Netlogon
- ✓ Monitoraggio eventi di autenticazione
- ✓ Isolamento Domain Controller



+ Fai una domanda



3. CVE-2021-34527 – PrintNightmare

Gravità: ● Critica

Categoria: Remote Code Execution / Privilege Escalation

Descrizione

Vulnerabilità nel Windows Print Spooler.

Consente a un attaccante di:

- installare driver malevoli
- ottenere privilegi SYSTEM
- eseguire codice remoto

Perché è pericolosa

- Il servizio Print Spooler è attivo di default
- Colpisce sia client che server

Impatto

- Compromissione completa della macchina
- Escalation rapida dei privilegi

Contromisure

- ✓ Patch di sicurezza Microsoft
- ✓ Disabilitare Print Spooler se non necessario
- ✓ Limitare installazione driver
- ✓ Policy di sicurezza restrittive



Fai una domanda



4. CVE-2019-0708 – BlueKeep

Gravità:  Critica

Categoria: Remote Code Execution

Descrizione

Vulnerabilità nel Remote Desktop Services (RDP).

Permette:

- esecuzione di codice remoto
- senza autenticazione
- potenziale comportamento worm-like

Perché è pericolosa

- Può colpire sistemi esposti a Internet
- Nessuna interazione dell'utente

Impatto

- Compromissione remota del sistema
- Rischio di worm simile a WannaCry

Contromisure


- ✓ Patch Microsoft
- ✓ Abilitare Network Level Authentication (NLA)
- ✓ Limitare RDP via firewall/VPN
- ✓ Monitoraggio accessi RDP



+ Fai una domanda



5. CVE-2021-36934 – HiveNightmare / SeriousSAM

Gravità:  Alta

Categoria: Privilege Escalation

Descrizione

Errore nei permessi dei file di registro:

- SAM
- SYSTEM
- SECURITY

Permette a utenti non privilegiati di:

- leggere hash delle password
- ottenere privilegi elevati offline

Perché è pericolosa

- Non richiede exploit complessi
- Facilita attacchi post-exploitation

Impatto

- Furto credenziali
- Escalation locale dei privilegi

Contromisure

- ✓ Aggiornamenti Microsoft
- ✓ Correzione ACL dei file di registro
- ✓ Eliminazione Shadow Copies
- ✓ Monitoraggio accessi ai file sensibili



+ | Fai una domanda



6. CVE-2022-30190 – Follina

Gravità: ● Critica

Categoria: Remote Code Execution

Descrizione

Vulnerabilità in Microsoft Support Diagnostic Tool (MSDT).

Consente:

- esecuzione di comandi
- aprendo un documento Word
- anche senza macro

Perché è pericolosa

- Bypass delle protezioni macro
- Facilmente sfruttabile via phishing

Impatto

- Compromissione tramite email
- Esecuzione di malware

Contromisure

- ✓ Patch Microsoft
- ✓ Disabilitare MSDT
- ✓ Restrizioni su documenti Office
- ✓ Formazione anti-phishing



+ Fai una domanda



[Fai l'upgrade a Go](#) x

✓ Restrizioni su documenti Office

✓ Formazione anti-phishing

7. CVE-2018-8639

Gravità: ● Alta

Categoria: Privilege Escalation

Descrizione

Vulnerabilità nel `Win32k.sys` (kernel Windows).

Consente:

- escalation locale dei privilegi
- ottenendo accesso kernel

Impatto

- Bypass dei controlli di sicurezza
- Persistenza avanzata

Contromisure

- ✓ Patch Microsoft
- ✓ Limitare account amministrativi
- ✓ Endpoint Detection (EDR)

Strategie generali di mitigazione (fondamentali)

+ Fai una domanda



Strategie generali di mitigazione (fondamentali)

Oltre alle patch specifiche:

✓ Aggiornamenti regolari

- Windows Update automatico
- Patch management centralizzato

✓ Principio del minimo privilegio

- Utenti standard
- Admin solo quando necessario

✓ Hardening del sistema

- Disabilitare servizi inutili
- Limitare protocolli legacy (SMBv1)

✓ Protezioni avanzate

- EDR/XDR
- IDS/IPS
- Firewall correttamente configurati

✓ Formazione utenti

- Riconoscere phishing
- Evitare allegati sospetti

INFINE CI HA SUGGERITO I MODI IN CUI POSSIAMO PROTEGGERCI DA QUESTE VULNERABILITÀ, COME CHIESTO ESPLICITAMENTE NEL PROMPT DA NOI SCRITTO.

SOMMA MASSIMO

