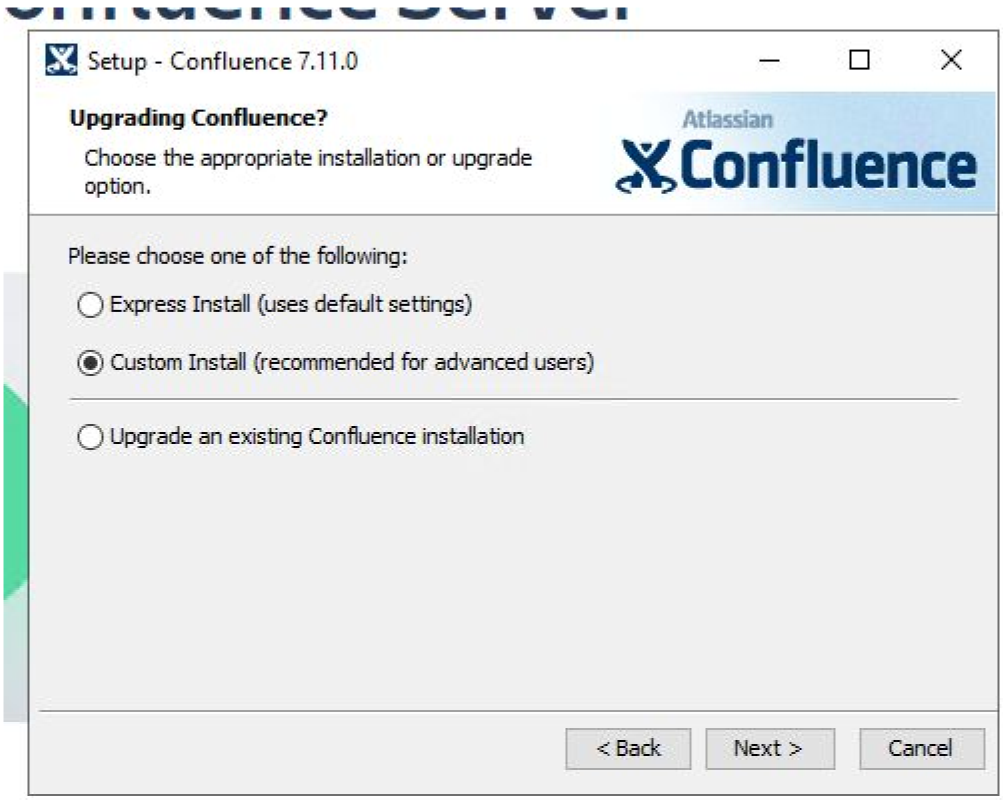
Atlassian Confluence Local Privilege Escalation

Below, we demonstrate how Atlassian Confluence is vulnerable to a DLL hijacking attack under certain conditions, allowing an unprivileged local attacker to take over the Confluence service. For more information on this attack vector generally, see our previous post.

To demonstrate this flaw, we first acquired the software installer from: https://www.atlassian.com/software/confluence/download.

During the installation we used the defaults at every step, except for the installation directory which we changed to `C:\Confluence` in order to demonstrate the permission misconfiguration. This directory can either be created through the installer GUI, or through `mkdir C:\Confluence`.



Setup - Confluence 7.11.0

Upgrading Confluence?

Choose the appropriate installation or upgrade option.

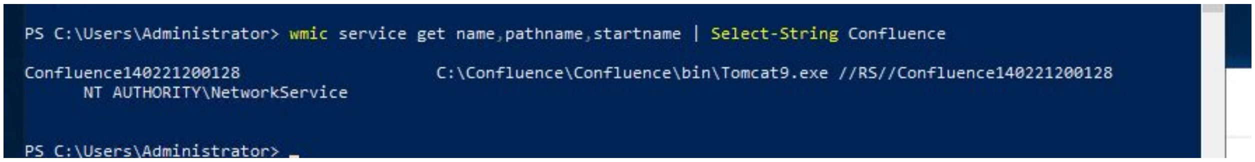
Please choose one of the following:

○ Express Install (uses default settings)

● Custom Install (recommended for advanced users)

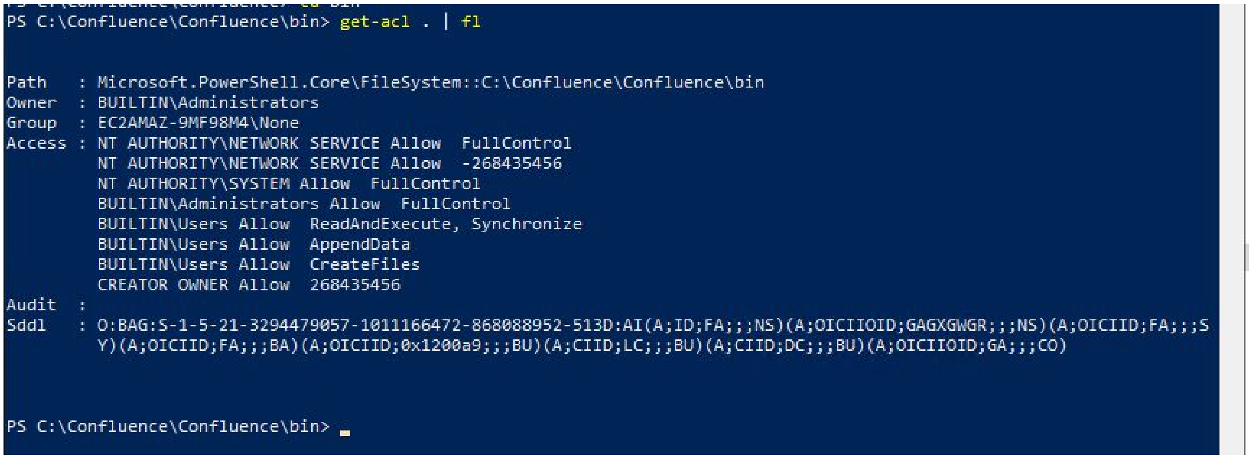
○ Upgrade an existing Confluence installation

If the installation is successful, we should find the service is registered as demonstrated by the following command:



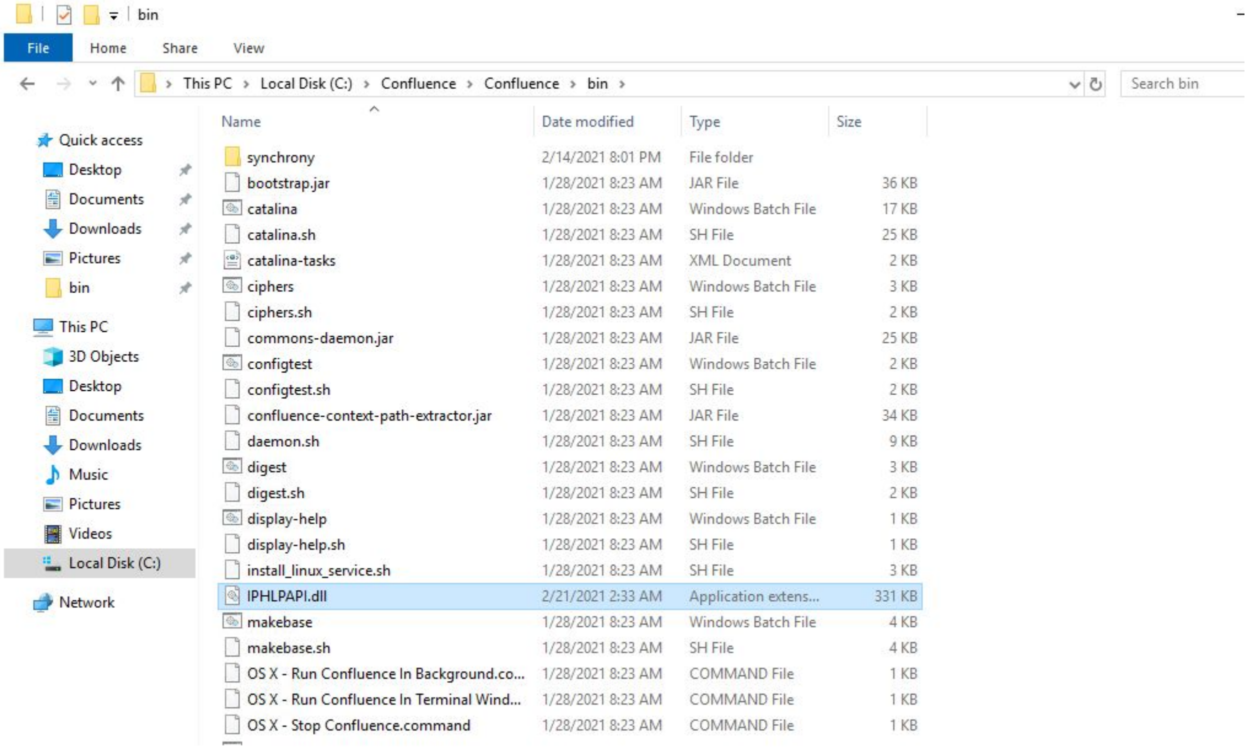
```
PS C:\Users\Administrator> wmic service get name,pathname,startname | Select-String Confluence

Confluence140221200128                C:\Confluence\Confluence\bin\Tomcat9.exe //RS//Confluence140221200128
      NT AUTHORITY\NetworkService


PS C:\Users\Administrator> _
```

Note the improper permissions, **`BUILTIN\Users Allow *`**, on the installation directory, which are inherited from the drive root. This gives any local user the ability to create arbitrary files in the installation directory, which we can then leverage in a DLL hijacking attack.



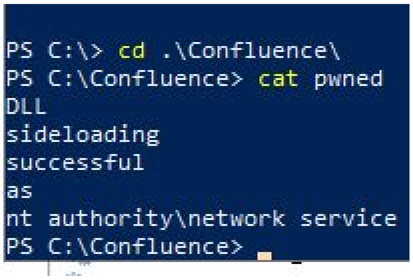
```
PS C:\Confluence\Confluence\bin> get-acl . | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Confluence\Confluence\bin
Owner  : BUILTIN\Administrators
Group  : EC2AMAZ-9MF98M4\None
Access : NT AUTHORITY\NETWORK SERVICE Allow  FullControl
         NT AUTHORITY\NETWORK SERVICE Allow  -268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  AppendData
         BUILTIN\Users Allow  CreateFiles
         CREATOR OWNER Allow  268435456
Audit  :
Sddl   : O:BAG:S-1-5-21-3294479057-1011166472-868088952-513D:AI(A;ID;FA;;;NS)(A;OICIIOID;GAGXGWGR;;;NS)(A;OICIID;FA;;;S
         Y)(A;OICIID;FA;;;BA)(A;OICIID;0x1200a9;;;BU)(A;CIID;LC;;;BU)(A;CIID;DC;;;BU)(A;OICIIOID;GA;;;CO)


PS C:\Confluence\Confluence\bin> _
```

To fully demonstrate the implications of this vulnerability, first create a new unprivileged user. Then, as this new user, download the provided IPHLPAPI.dll file (https://drive.google.com/drive/folders/1XgsHgK-x5YmrzzSxoEHakcui6MLnYJ4b?usp=sharing). Note how the user has permissions to add the poisoned DLL to the installation directory.



Name	Date modified	Type	Size
synchrony	2/14/2021 8:01 PM	File folder	
bootstrap.jar	1/28/2021 8:23 AM	JAR File	36 KB
catalina	1/28/2021 8:23 AM	Windows Batch File	17 KB
catalina.sh	1/28/2021 8:23 AM	SH File	25 KB
catalina-tasks	1/28/2021 8:23 AM	XML Document	2 KB
ciphers	1/28/2021 8:23 AM	Windows Batch File	3 KB
ciphers.sh	1/28/2021 8:23 AM	SH File	2 KB
commons-daemon.jar	1/28/2021 8:23 AM	JAR File	25 KB
configtest	1/28/2021 8:23 AM	Windows Batch File	2 KB
configtest.sh	1/28/2021 8:23 AM	SH File	2 KB
confluence-context-path-extractor.jar	1/28/2021 8:23 AM	JAR File	34 KB
daemon.sh	1/28/2021 8:23 AM	SH File	9 KB
digest	1/28/2021 8:23 AM	Windows Batch File	3 KB
digest.sh	1/28/2021 8:23 AM	SH File	2 KB
display-help	1/28/2021 8:23 AM	Windows Batch File	1 KB
display-help.sh	1/28/2021 8:23 AM	SH File	1 KB
install_linux_service.sh	1/28/2021 8:23 AM	SH File	3 KB
IPHLPAPI.dll	2/21/2021 2:33 AM	Application extens...	331 KB
makebase	1/28/2021 8:23 AM	Windows Batch File	4 KB
makebase.sh	1/28/2021 8:23 AM	SH File	4 KB
OS X - Run Confluence In Background.co...	1/28/2021 8:23 AM	COMMAND File	1 KB
OS X - Run Confluence In Terminal Wind...	1/28/2021 8:23 AM	COMMAND File	1 KB
OS X - Stop Confluence.command	1/28/2021 8:23 AM	COMMAND File	1 KB

From here, restart the computer, or restart the Confluence service as an administrator. The payload contained in the DLL will then execute and the evidence of that can be found in the text file **`C:\Confluence\pwned`**.



```
PS C:\> cd .\Confluence\
PS C:\Confluence> cat pwned
DLL
sideloading
successful
as
nt authority\network service
PS C:\Confluence> _
```

Although **`Network Service`** may not seem like a highly-privileged account, this vulnerability would clearly allow any user to gain control of the Confluence service and any sensitive data it may have access to. In addition, there appear to be publicly documented techniques that could allow an attacker to further escalate from **`Network Service`** to **`Local System`** (the fully privileged administrative user), which would clearly be a significant risk to a customer's infrastructure generally.