

Das BSI warnt: Log4j Schwachstelle. Scanning mit Ansible

Thomas Baumann tiri GmbH

Ansible Anwender Treffen 15.02.2022

© tiri GmbH

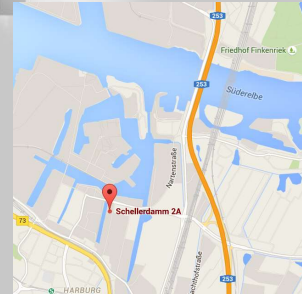
1



Hamburg

2

Im Herzen des Harburger Hafens.



3

Im Herzen des Harburger Hafens.

- „tiri“ wurde 2008 durch Thomas Baumann gegründet.
- tiri GmbH hat zahlreiche renommierte Kunden (bundesweit, teilweise auch DACH-Region).
- Es werden hauptsächlich Kunden aus Hamburg und Norddeutschland betreut, teilweise mit Vor-Ort-Service, viele Kunden auch Remote überregional.
- tiri GmbH hat ihren Sitz zentral im Herzen des Harburger Hafens in einem wunderschönen denkmalgeschützten Kaufmannhaus (1845)
- Nahe des ICE Bahnhofs Hamburg-Harburg und damit für Kunden und Mitarbeiter optimal erreichbar.



4



5

A

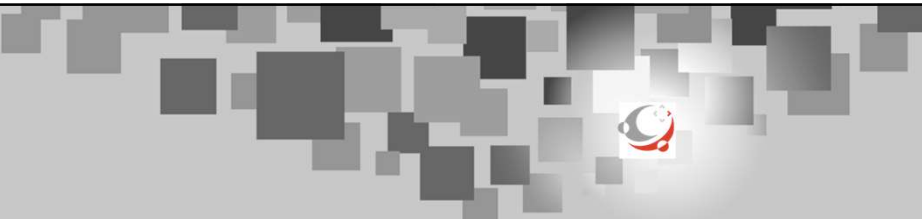
Das BSI warnt: Log4j Schwachstelle.
Scanning mit Ansible

Thomas Baumann

Ansible Anwender Treffen 15.02.2022

© tiri GmbH

6



- Was ist Log4j ?
- Was ist eine Zero-Day Schwachstelle?
- Was wurde als Verwundbarkeit in Log4j entdeckt?

© tiri GmbH

7 **tiri** Member of ACP Group

7

Ausgangsposition



twitter.com/malwaretechblog/status/1469290238702874625?lang=de

  **Thread**

 **Marcus Hutchins** 
@MalwareTechBlog

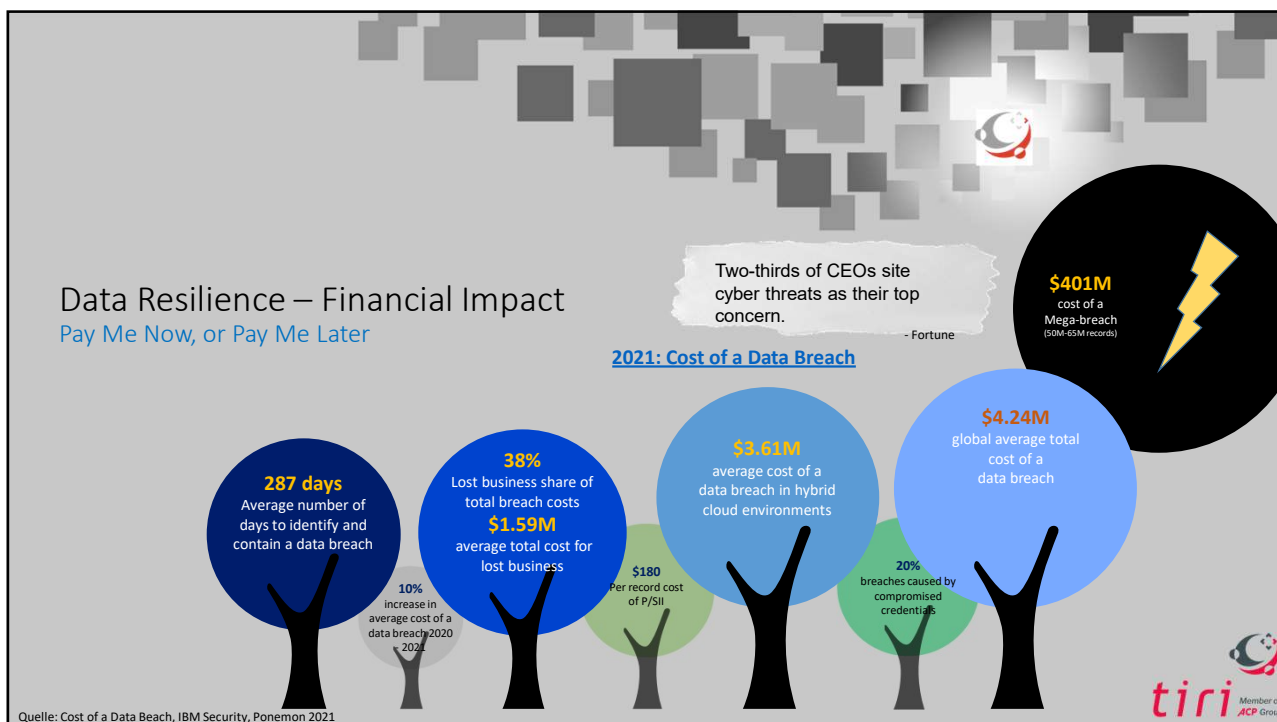
In the case of Minecraft, attackers were able to get remote code execution on Minecraft Servers by simply pasting a a short message into the chat box.

1:57 nachm. · 10. Dez. 2021 · Twitter Web App

© tiri GmbH

8 **tiri** Member of ACP Group

8



9

Historie

Exploiting JNDI Injections in Java
By Michael Stepankin
January 3, 2019

<https://www.veracode.com/blog/research/exploiting-jndi-injections-java>

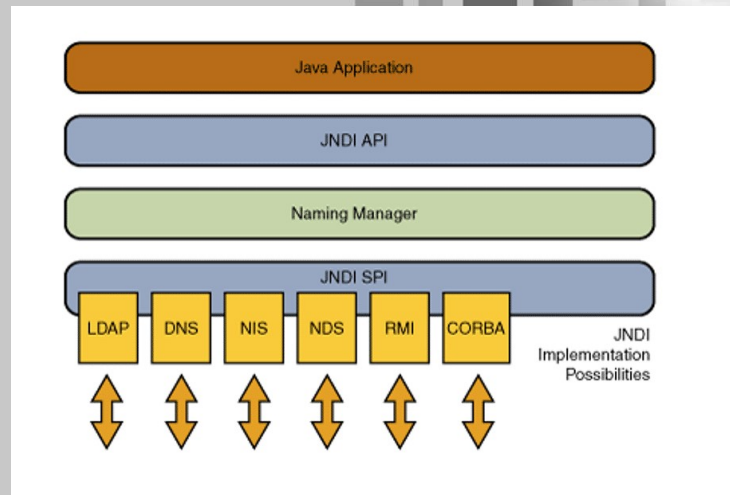
black hat USA 2016
A JOURNEY FROM JNDI/LDAP MANIPULATION TO REMOTE CODE EXECUTION DREAM LAND
Alvaro Muñoz (@pwntester)
Oleksandr Mirosh

<https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE-wp.pdf>

© tiri GmbH

11

JNDI Implementation



Quelle: <https://docs.oracle.com/javase/tutorial/jndi/overview>

© tiri GmbH

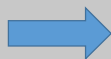
13

tiri Member of ACP Group

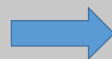
13

JNDI Implementation

Module java.naming
module java.naming
Defines the Java Naming and Directory Interface (JNDI) API.
Common standard JNDI environment properties that may be supported by JNDI providers are defined and documented in Context. Specific JNDI provider implementations may also support other environment or system properties, which are specific to their implementation.



Module java.naming
Package javax.naming.spi
package javax.naming.spi
Provides the means for dynamically plugging in support for accessing naming and directory services through the javax.naming and related packages.



Module java.naming
Package javax.naming.spi
Class NamingManager
This class contains methods for creating context objects and objects referred to by location information in the naming or directory service.

Quelle: <https://docs.oracle.com/en/java/javase/17/>

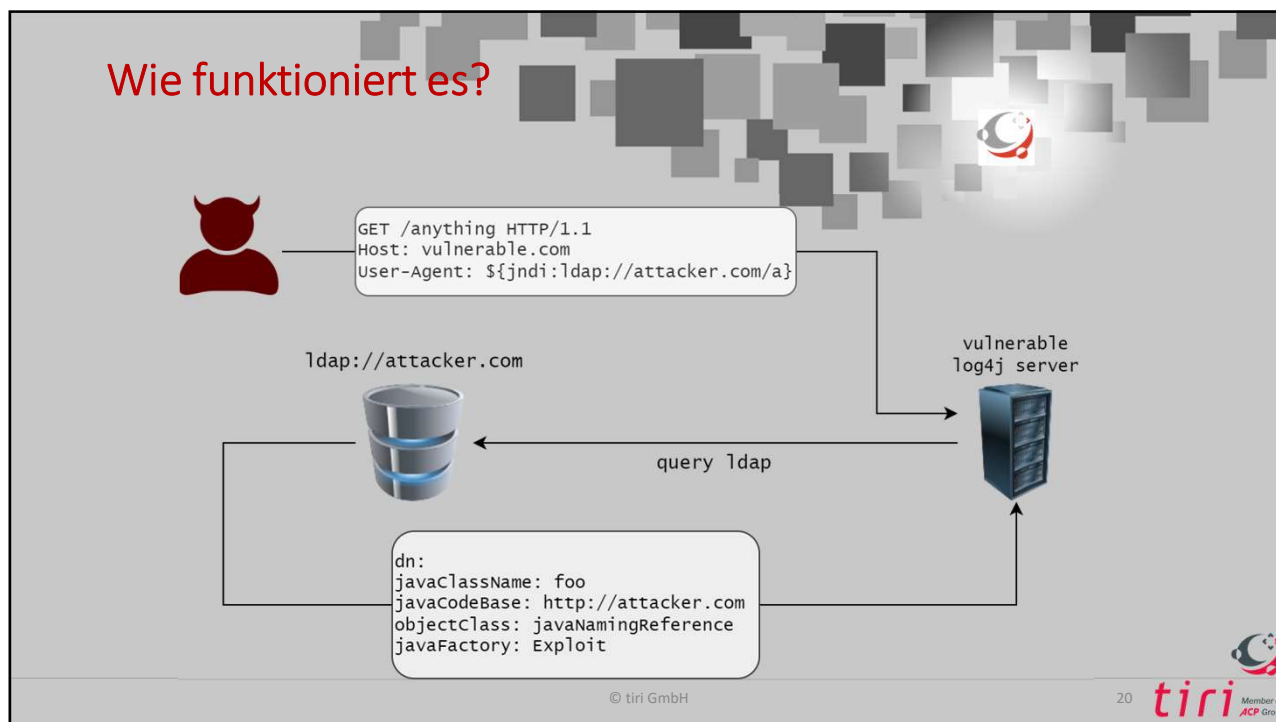
© tiri GmbH

15

tiri Member of ACP Group

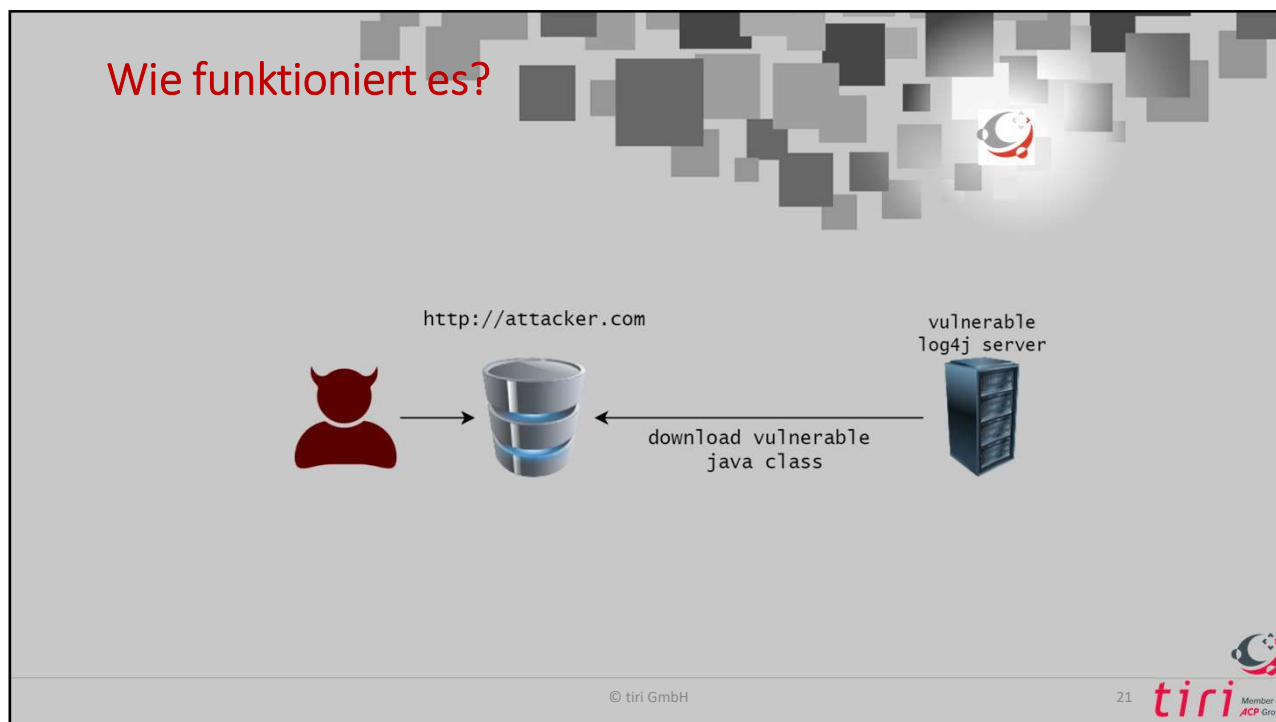
15

Wie funktioniert es?

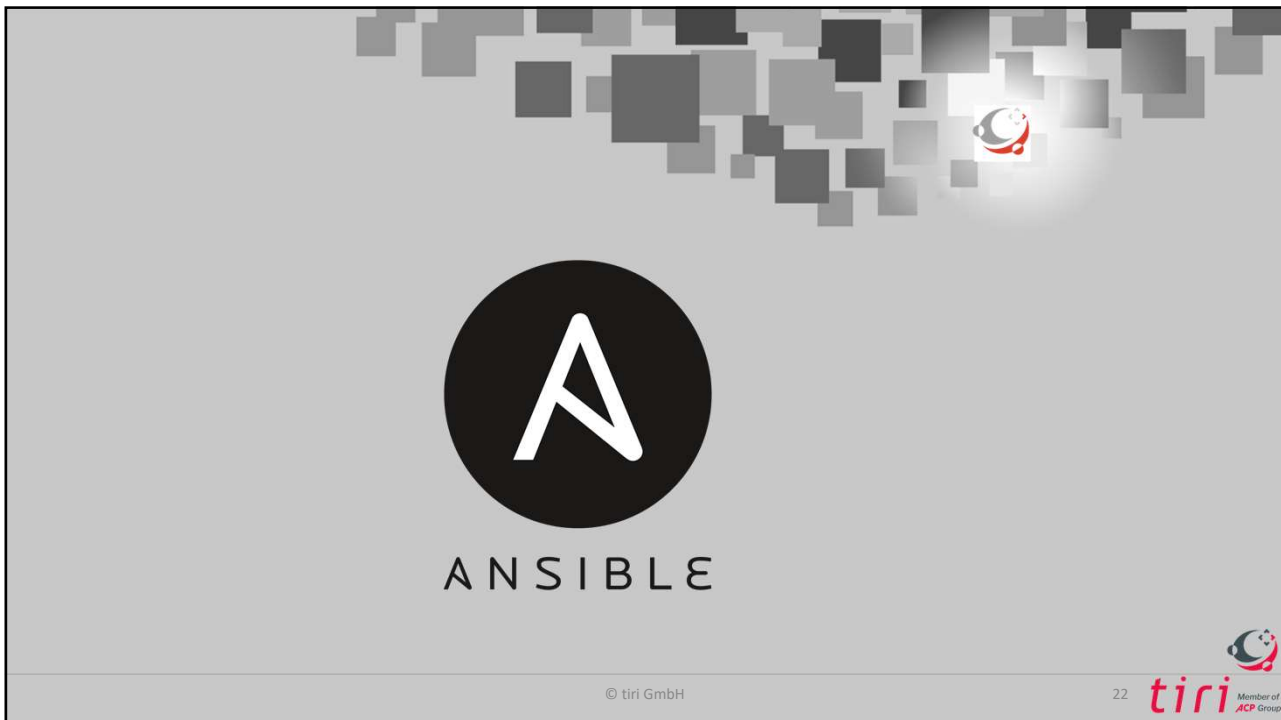


20

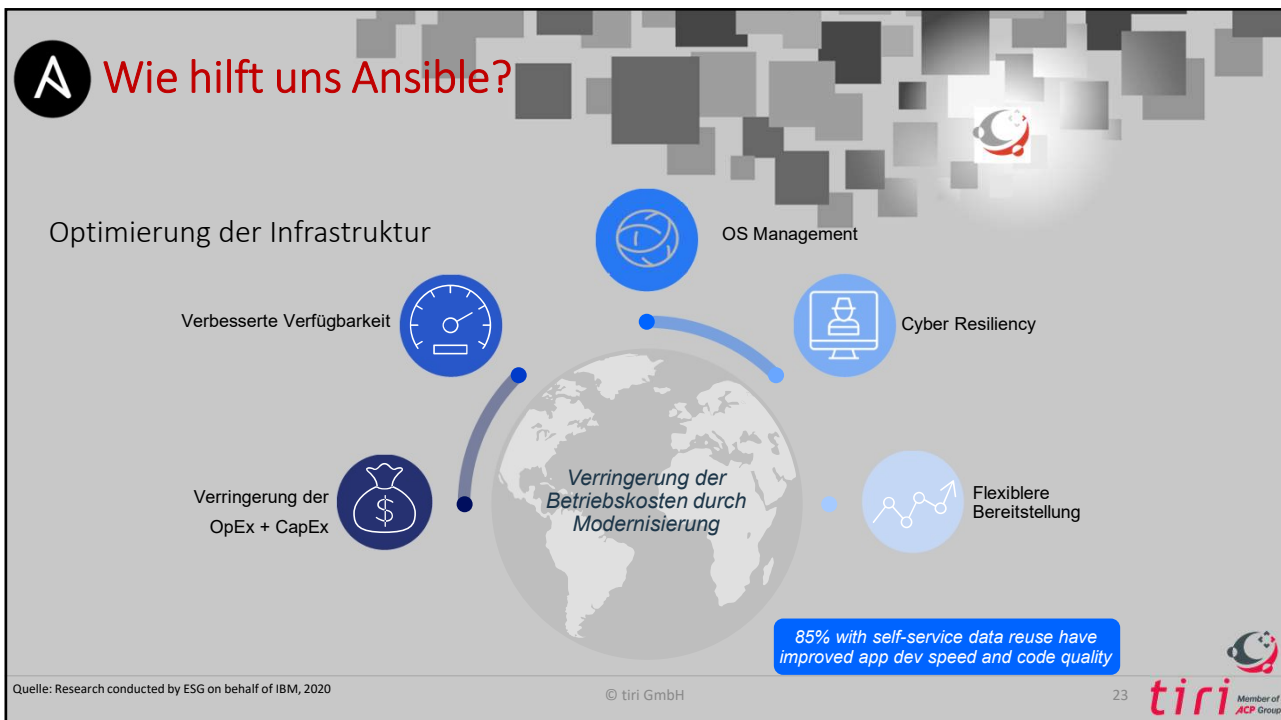
Wie funktioniert es?



21



22



23

A Wie hilft uns Ansible?





Powerful
Orchestrate complex processes at enterprise scale.



Simple
Simplify automation creation and management across multiple domains.



Agentless
Easily integrate with hybrid environments.

- Ansible Automation Platform AAP2

© tiri GmbH

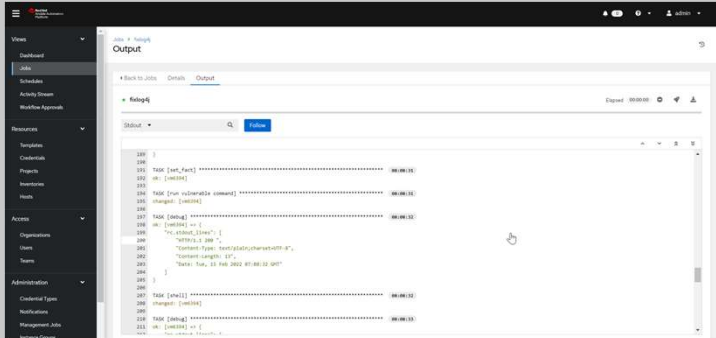
24 **tiri** Member of ACP Group

24

A Wie hilft uns Ansible?



Live Demo



© tiri GmbH

25 **tiri** Member of ACP Group

25

A Wie hilft uns Ansible?

Live Demo

```
switchboard /usr/local/lib/python2.7/dist-packages/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
switchboard from cryptography import x509
switchboard console public key: 093CR7T1N3ouXuCuaU1In8B5b1YsX11AqQwRwTck=
switchboard 2022-02-24T11:25:44+0000 [-] Loading switchboard.tac...
switchboard 2022-02-24T11:25:45+0000 [switchboard#info] Canarytokens switchboard started
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Email
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel TwilioSMS
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Webhook
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel DNS
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel HTTP
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Impur
switchboard 2022-02-24T11:25:45+0000 [channel_input_linkedin#info] Started channel LinkedIn
switchboard 2022-02-24T11:25:45+0000 [channel_input_bitcoin#info] Started channel Bitcoin
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Bitcoin
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel SMTP
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Kubeconfig
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel MySQL
switchboard 2022-02-24T11:25:45+0000 [channel#info] Started channel Wireguard
switchboard 2022-02-24T11:25:45+0000 [twisted.web.client.HTTPClientFactory#info] Starting factory <HTTPClientFactory: https://check.torproject.org/exit-addresses>
switchboard 2022-02-24T11:25:45+0000 [-] Loaded
switchboard 2022-02-24T11:25:45+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 19.10.0 (/usr/bin/python 2.7.12) starting up.
switchboard 2022-02-24T11:25:45+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor
switchboard 2022-02-24T11:25:45+0000 [-] DNSServerFactory starting on 53
switchboard 2022-02-24T11:25:45+0000 [channel_dns.DNSServerFactory#info] Starting factory <channel_dns.DNSServerFactory object at 0x7f2079b34990>
switchboard 2022-02-24T11:25:45+0000 [-] DNSDatagramProtocol starting on 53
switchboard 2022-02-24T11:25:45+0000 [-] Starting protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f2079b34a90>
switchboard 2022-02-24T11:25:45+0000 [-] Site starting on 8083
```

© tiri GmbH

26

tiri Member of ACP Group

26



Weitere Aktionen

Workshop Security & Threat Intelligence Monitoring

© tiri GmbH

28

tiri Member of ACP Group

28



Wir stellen ein | Wir freuen uns auf Sie !

Linux Systemoptimierung | Support | Betrieb | Security

tiri GmbH | Member of ACP Group
Schellerdamm 2a
D – 21079 Hamburg
www.tiri.li
TEL: +49 40 52 47 507-0

© tiri GmbH

29  Member of ACP Group

29