REPORT

INFORMATION GATHERING

IP Address Resolution

Resolved IP Address: 3.74.31.225

WHOIS Lookup

Domain Information

- Domain Name: infopark.com

- Registrar: GANDI SAS

- Registrar IANA ID: 81

- Creation Date: 1996-12-10T04:00:00Z

- Last Updated: 2024-08-02T16:33:06Z

- Expiration Date: 2024-12-09T05:00:00Z

- Domain Statuses: clientTransferProhibited

Registrant Information

- Name: REDACTED FOR PRIVACY

- Organization: JustRelate Deutschland GmbH

- Address: REDACTED FOR PRIVACY

- City: REDACTED FOR PRIVACY

- State: Not Available

- Postal Code: REDACTED FOR PRIVACY

- Country: GERMANY

- Phone: Not Available

- Fax: Not Available

- Email: 308096e6d1a4a8e65953dc48a85709ee-49734315@contact.gandi.net

Administrative Contact

- Name: REDACTED FOR PRIVACY

- Organization: REDACTED FOR PRIVACY

- State: REDACTED FOR PRIVACY

- Country: REDACTED FOR PRIVACY

Technical Contact

- Name: REDACTED FOR PRIVACY

- Organization: REDACTED FOR PRIVACY

- State: REDACTED FOR PRIVACY

- Country: REDACTED FOR PRIVACY

Name Servers

- NS-1256.AWSDNS-29.ORG, NS-1583.AWSDNS-05.CO.UK, NS-392.AWSDNS-49.COM, NS-878.AWSDNS-45.NET

Additional Information

- Domain Protection: The domain is safeguarded under multiple prohibitive statuses.

InternetDB Information

InternetDB Information for IP: 3.74.31.225

Open Ports:

  - 80

  - 443

CPEs:

Hostnames:

  - ec2-3-74-31-225.eu-central-1.compute.amazonaws.com

Tags:

  - cloud

Vulnerabilities: None

Geolocation Lookup

IP Information

- IP: 3.74.31.225

- Hostname: ec2-3-74-31-225.eu-central-1.compute.amazonaws.com

- City: Frankfurt am Main

- Region: Hesse

- Country: DE

- Location: 50.1155,8.6842

- Organization: AS16509 Amazon.com, Inc.

- Postal: 60306

- Timezone: Europe/Berlin

Shodan Information

Shodan Information for IP: 3.74.31.225

Organization: A100 ROW GmbH

Operating System: None

ISP: Amazon.com, Inc.

Country: Germany

City: Frankfurt am Main

Latitude: 50.11552

Longitude: 8.68417

Open Ports:

Port: 80

Service: AWS ELB

Version: 2.0

Banner: HTTP/1.1 301 Moved Permanently

Server: awselb/2.0

Date: Mon, 26 Aug 2024 13:52:05 GMT

Content-Type: text/html

Content-Length: 134

Connection: keep-alive

Location: https://infopark.de:443/

Port: 443

Service: AWS ELB

Version: 2.0

Banner: HTTP/1.1 301 Moved Permanently

Server: awselb/2.0

Date: Mon, 26 Aug 2024 20:07:21 GMT

Content-Type: text/html

Content-Length: 134

Connection: keep-alive

Location: https://www.justrelate.com:443/

Conclusion

Shodan identified 2 open ports, which could serve as potential entry points for attackers. It is recommended to review these open ports and secure or close them if they are not needed. Disabling unnecessary services can minimize exposure to threats.

WHOIS lookup provided detailed information about the domain ownership. This information can be used to understand the entity behind the domain and assess potential risks associated with it.

The IP is located in DE, which could indicate the origin of the services and provide insights into potential regional threats.

The system is detected as vulnerable. Immediate action is advised to mitigate the identified risks.