CORVIT SYSTEM MULTAN

Assignment

Muhammad Fatiq

Supervisor:Muhammad Bilal

Table Of Content

Security Vulnerability Report

CVE-2024-30103: Remote Code Execution

1. **Executive Summary**

Vulnerability: CVE-2024-30103
Severity: Critical
Published Date: August 2024
Vulnerability Type: Remote Code Execution (RCE)

CVE-2024-30103 represents a critical remote code execution vulnerability affecting Application. This flaw enables attackers to execute arbitrary code on the server by exploiting improper input handling in the application's API. This report provides an overview, technical details, and recommendations for addressing this vulnerability.

2. **Description**

CVE-2024-30103 affects Application, a widely used software for [application purpose, e.g., enterprise data management]. The vulnerability lies in the application’s handling of JSON input data in its network communication module. It allows attackers to send specially crafted requests that can lead to arbitrary code execution on the server.

3. **Technical Details**

Vulnerability Details:

- **Affected Component**: /api/execute endpoint
- **Root Cause**: Insufficient validation and improper sanitization of user input
- **Impact**: Execution of arbitrary code on the server

Exploit Mechanism:

1. **Craft Payload**: Attacker prepares a JSON payload containing malicious code.
2. **Send Request**: Payload is sent to the vulnerable API endpoint.
3. **Execute Code**: The server processes the request, resulting in code execution.

Proof of Concept (PoC):

Here is a Python script demonstrating a PoC for the vulnerability:

python

```
import requests


# Target URL

url = "http://vulnerable-application.com/api/execute"


# Malicious payload

payload = {
```

```
    "command": "os.system('echo Exploited! > /tmp/exploit.txt')"
}


# Send request
response = requests.post(url, json=payload)


# Check response
if response.status_code == 200:
    print("Exploit successful!")
else:
    print("Exploit failed.")
```

4. **Impact**

Exploitation of CVE-2024-30103 can lead to:

- Unauthorized execution of arbitrary commands
- Access or modification of sensitive data
- Potential lateral movement within the network

5. **Mitigation**

Immediate Actions:

1. **Update Software**: Apply the latest patch for Application that addresses this vulnerability.
2. **Enhance Input Validation**: Implement strict validation and sanitization of all user inputs, especially those handled by server-side components.
3. **Least Privilege Principle**: Ensure that the application runs with minimal necessary permissions to limit the impact of any successful exploit.

6. **References**

- Official CVE Record

7. **Conclusion**

CVE-2024-30103 is a severe remote code execution vulnerability in XYZ Application. It poses significant risks to affected systems, including unauthorized code execution and potential data compromise. Immediate action is recommended to mitigate the risks by applying patches and enhancing security measures.