مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Apache MINA

Tracking #:432316672

Date:26-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache MINA, a popular network application framework. This vulnerability could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-52046**
- CVSS Score 10.0 (Critical)
- The vulnerability exists in the ObjectSerializationDecoder component, which lacks necessary security checks when processing serialized data. Attackers can exploit this by sending specially crafted malicious serialized data, potentially leading to Remote Code Execution (RCE).
- The vulnerability specifically affects applications using the IoBuffer#getObject() method, which is called when adding a ProtocolCodecFilter instance using the ObjectSerializationCodecFactory class in the filter chain
- Successful exploitation could allow attackers to execute arbitrary code on vulnerable systems, potentially gaining complete control

Affected Versions:

- Apache MINA 2.0 through 2.0.26
- Apache MINA 2.1 through 2.1.9
- Apache MINA 2.2 through 2.2.3

Mitigations:

1. Upgrade to the patched versions:
    - Apache MINA 2.0.27
    - Apache MINA 2.1.10
    - Apache MINA 2.2.4

2. After upgrading, explicitly define allowed classes for deserialization using one of the new methods:
    - accept(ClassNameMatcher classNameMatcher)
    - accept(Pattern pattern)
    - accept(String... patterns)

3. Review and limit the use of IoBuffer#getObject() in your applications
4. Implement additional security measures such as input validation and network segmentation

Important Notes:

- Upgrading alone is not sufficient; configuration changes are required after updating
- The FtpServer, SSHd, and Vysper sub-projects are not affected by this vulnerability
- By default, the updated decoder will reject all classes unless explicitly allowed

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Apache MINA.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-52046