

## Apache RocketMQ Remote Command Execution Vulnerability

### Open source software actively exploited

<https://lists.apache.org/thread/1s8j2c8kogthpv3060yddk03zq0pxyp>  
 CVEs: CVE-2023-33246

RocketMQ versions 5.1.0 and below are vulnerable to Arbitrary Code Injection. Broker component of RocketMQ is leaked on the extranet and lack permission verification. An attacker can exploit this vulnerability by using the update configuration function to execute commands or by forging the RocketMQ protocol content. CVE-2023-33246 is reportedly being exploited in the wild. Additionally, proof-of-concept (PoC) code is publicly available.

**Background** RocketMQ is a distributed messaging and streaming platform. It was open sourced by Alibaba in 2012. In 2016, Alibaba donated RocketMQ to the Apache Software Foundation and is Apache Software Foundation announced it as a Top-level project. According to the vendor, RocketMQ has become the industry standard for financial-grade reliable business messages and is widely used in Internet, big data, mobile Internet, IoT, and other fields.

**Announced** May 23, 2023: RocketMQ team released patch and advisory about the vulnerability  
<https://lists.apache.org/thread/1s8j2c8kogthpv3060yddk03zq0pxyp>

Jun 22, 2023: FortiGuard Labs released a Threat signal on CVE-2023-33246.  
<https://www.fortiguard.com/threat-signal-report/5203>

**Latest Developments** 29 June, 2023: FortiGuard Labs released an IPS signature to detect and block attacks leveraging CVE-2023-33246 and has blocked attack attempts on upto 1000+ unique IPS devices since the release.

To mitigate the risk completely, users are recommended to upgrade to version 5.1.1 or above for (RocketMQ 5.x) and 4.9.6 or above for using (RocketMQ 4.x).  
<https://lists.apache.org/thread/1s8j2c8kogthpv3060yddk03zq0pxyp>

06 Sept, 2023: CISA added CVE-2023-33246 to its known exploited catalog list (KEV)


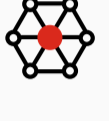

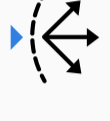

## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation



### IPS

Detects and blocks attack attempts related to Apache RocketMQ Remote Command Execution Vulnerability (CVE-2023-33246)

 FortiGate DB 24.593	 FortiSASE DB 24.593	 FortiNDR DB 24.593	 FortiADC DB 24.593	 FortiProxy DB 24.593
---	---	--	--	--

### Web App Security

Detects and blocks attack attempts related to Apache RocketMQ Remote Command Execution Vulnerability (CVE-2023-33246)

 FortiWeb DB 0.00353	 FortiADC DB 1.00043
---	---

### Installation

#### Post-execution

  
 FortiEDR  
 v4.0+


### C2

### Action



## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

### Outbreak Detection

  
 FortiAnalyzer  
 DB 2.00010

### Threat Hunting

 FortiAnalyzer v6.4+	 FortiSIEM v6.5+
---	---

### Content Update


  
 FortiSIEM  
 DB 409

## RESPOND

Develop containment techniques to mitigate impacts of security events:



### Automated Response

Services that can automatically respond to this outbreak.

  
 FortiXDR

### Assisted Response Services

Experts to assist you with analysis, containment and response activities.



 Incident Response	 FortiRecon: ACI
--	--

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

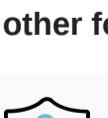
### NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
---	---

### End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

  
 Security Awareness & Training

## IDENTIFY

Identify processes and assets that need protection:

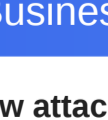
### Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

  
 Security Rating

### Business Reputation

Know attackers next move to protect against your business branding.

  
 FortiRecon: EASM

## Additional Resources

Apache Advisory <https://lists.apache.org/thread/1s8j2c8kogthpv3060yddk03zq0pxyp>

Learn more about [FortiGuard Outbreak Alerts](#)