

## Oracle WebLogic Server Vulnerability

### Attackers target vulnerable WebLogic servers

<https://www.oracle.com/security-alerts/cpujan2023.html>  
 CVEs: CVE-2023-21839

Known exploited vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware. This vulnerability allows an unauthenticated attacker with network access via T3, IIOP, to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data on the Oracle WebLogic Server and the confidentiality impact of the vulnerability is rated as "High".

**Background** Oracle WebLogic Server is a unified and extensible platform for developing, deploying and running enterprise applications, such as Java, for on-premises and in the cloud. In the previous years, we have seen some other vulnerabilities namely, CVE-2018-3252, CVE-2020-14645 and CVE-2020-2883 in the Oracle WebLogic Server. FortiGuard Labs provided IPS signature protections against these flaws in 2018 and 2020 respectively. According to the IPS telemetry, we can see the attacks are still active in 2023. Go to Additional Resources for full Threat Encyclopedia.

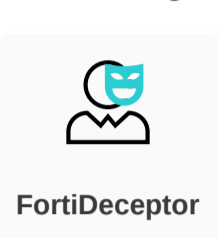
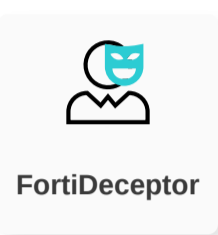






**Announced** January, 2023: Oracle released a critical patch update advisory. The affected versions of Oracle WebLogic server include 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0.  
<https://www.oracle.com/security-alerts/cpujan2023.html>

**Latest Developments** May 1, 2023: CISA added CVE-2023-21839 in CISA's Known Exploited Vulnerabilities Catalog (KEV).  
 May 2, 2023: FortiGuard Labs released a Threat Signal on the vulnerability  
<https://www.fortiguard.com/threat-signal-report/5154>

FortiGuard Labs has released an IPS signature to detect and block attack attempts targeting vulnerable Oracle WebLogic Server and also recommends organizations to review and patch affected versions as recommended in the vendor advisory.

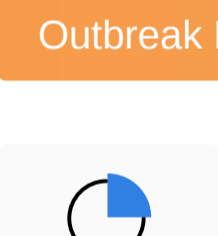
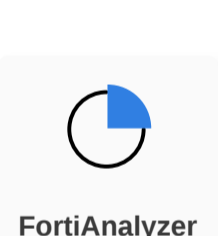

## PROTECT

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

- Reconnaissance**
  - Lure**  
 Detects attack attempts related to Oracle WebLogic Server Vulnerability and prevents lateral movement on the network segment  
  
 FortiDeceptor  
 v3.3+
  - Decoy VM**  
 Detects attack attempts related to Oracle WebLogic Server Vulnerability and prevents lateral movement on the network segment  
  
 FortiDeceptor  
 v3.3+
- Weaponization**
- Delivery**
- Exploitation**
  - IPS**  
 Detects and blocks attack attempts related to Oracle WebLogic Server Vulnerability (CVE-2023-21839)  
 FortiGate DB 23.547
  FortiSASE DB 23.547
  FortiNDR DB 23.547
  FortiADC DB 23.547
  FortiProxy DB 23.547
- Installation**
  - Post-execution**  
 Detects and blocks post exploitation activity related to known and unknown malware  
  
 FortiEDR  
 v4.0+
- C2**
- Action**

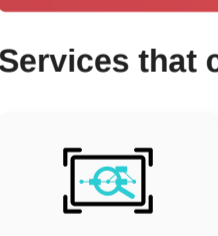
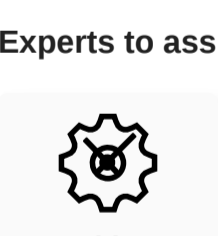
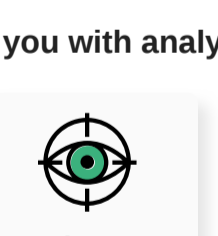
## DETECT

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

- Outbreak Detection**  
  
 FortiAnalyzer  
 DB 2.00002
- Threat Hunting**  
  
 FortiAnalyzer  
 v6.4+
- Content Update**  
  
 FortiSIEM  
 DB 315

## 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

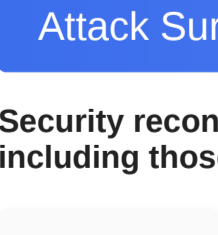
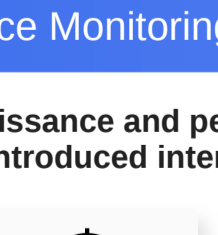
## RECOVER

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

- InfoSec Services**  
 Security readiness and awareness training for SOC teams, InfoSec and general employees.  
  
 Response Readiness

## IDENTIFY

Identify processes and assets that need protection:

- Attack Surface Monitoring (Inside & Outside)**  
 Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.  
 Security Rating
  FortiRecon: EASM

## Additional Resources

- The Hacker News <https://thehackernews.com/2023/05/active-exploitation-of-tp-link-apache.html>
- CISA KEV <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- FortiGuard IPS for CVE-2018-3252 <https://www.fortiguard.com/encyclopedia/ips/47154>
- FortiGuard IPS for CVE-2020-14645 & CVE-2020-2883 <https://www.fortiguard.com/encyclopedia/ips/49001>

Learn more about [FortiGuard Outbreak Alerts](#)