



Oracle WebLogic Server Vulnerability

Attackers target vulnerable WebLogic servers

<https://www.oracle.com/security-alerts/cpujan2023.html>

CVEs: CVE-2023-21839, CVE-2017-3506

Known exploited vulnerabilities in the Oracle WebLogic Server. The vulnerabilities allows an unauthenticated attacker with network to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data on the Oracle WebLogic Server and attacker may further use it to deploy malware such as cryptocurrency miners.

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.

Latest Developments

FortiGuard Labs has available IPS signatures to detect and block attack attempts targeting vulnerable Oracle WebLogic Server (CVE-2017-3506, CVE-2023-21839) and also recommends organizations to review and patch affected versions as recommended in the vendor advisory.

June 3, 2024: CISA added an Oracle WebLogic flaw (CVE-2017-3506) to its Known Exploited Vulnerabilities (KEV) catalog.

May 30, 2024: Trend Micro reported that a threat actor 8220 Gang was observed exploiting Oracle WebLogic server CVE-2017-3506 along with CVE-2023-21839 to deploy cryptocurrency miner.

https://www.trendmicro.com/en_us/research/24/e/decoding-8220-latest-obfuscation-tricks.html

May 2, 2024: FortiGuard Labs released a Threat Signal on the vulnerability

<https://www.fortiguard.com/threat-signal-report/5154>

May 1, 2024: CISA added CVE-2023-21839 in CISA's Known Exploited Vulnerabilities Catalog (KEV).

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 leveraging the vulnerability



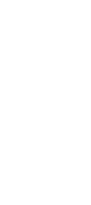
FortiADC

DB 23.547



FortiGate

DB 23.547



FortiNDR

DB 23.547



FortiProxy

DB 23.547



FortiSASE

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:

IOC



FortiAnalyzer



FortiSOCaaS



FortiSIEM

Outbreak Detection

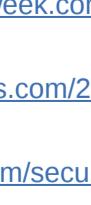


FortiAnalyzer

DB 2.00002



FortiSIEM



FortiSOAR

DB 315

Threat Hunting



FortiAnalyzer

v6.4+

Playbook

FortiSOAR

Response Readiness

Security Awareness Training

InfoSec Services

Security Readiness

Incident Response

Response Readiness

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Response Readiness

Assisted Response Services

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

Incident Response

Containment, Recovery and Remediation

Containment, Recovery and Remediation