FORTINET

OUTBREAK ALERTS

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 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: FortiGuards 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	FortiGate	FortiNDR	FortiProxy	FortiSASE
DB 23.547	*DB 23.547*	*DB 23.547*	*DB 23.547*	*DB 23.547*

Installation

Post-execution

Detects and blocks post exploitation activity related to known and unkown 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	FortiSIEM	FortiSOAR
DB 2.00002	*DB 315*	

Threat Hunting

FortiAnalyzer
v6.4+

Playbook

FortiSOAR

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

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

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 Hardening

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

Security Rating

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
Security Week	https://www.securityweek.com/cisa-warns-of-attacks-exploiting-old-oracle-weblogic-vulnerability/
The Hacker News	https://thehackernews.com/2024/06/oracle-weblogic-server-cs-command.html
Oracle Advisory 2023	https://www.oracle.com/security-alerts/cpujan2023.html
Oracle Advisory 2017	https://www.oracle.com/security-alerts/cpujan2017.html

Learn more about FortiGuard Outbreak Alerts

FORTINET