

|  |
| --- |
| Oracle WebLogic Server Remote Code Execution Vulnerability (CVE-2024-21216) |
| ■ Circular No. | **NS-2024-0031-1** | ■ Date of issue |  **2024-11-08** |
| ■ Vulnerability hazard | **An attacker could exploit this vulnerability to enable remote code execution.** |
| ■ TAG | Oracle WebLogic, CVE-2024-21216, Remote Code Execution |



|  |
| --- |
| © 2024 NSFOCUS |

1. Vulnerability Overview

Recently, NSFOCUS CERT detected that Oracle issued a security announcement and fixed the deserialization vulnerability in WebLogic Server (CVE-2024-21216). Since WebLogic does not strictly filter incoming data through the T3/IIOP protocol, when the T3/IIOP protocol is enabled, an unauthenticated remote attacker sends a special request to the server through the T3/IIOP protocol to execute arbitrary code on the target system. The CVSS rating is 9.8. At present, it has been found to be used in the wild. Please take measures for protection as soon as possible.

WebLogic is a Java EE application server developed by BEA Systems and now owned by Oracle. It provides a complete Java EE platform and a wide range of services and functions, such as Web server, EJB container, JMS message queue, transaction management, security, etc., with high scalability and stability.

NSFOCUS has successfully replicated this vulnerability:



Reference link:

https://www.oracle.com/security-alerts/cpuoct2024.html

1. Scope of Influence

**Affected version**

* Weblogic 12.2.1.4.0
* Weblogic 14.1.1.0.0

Note: The above is the influence scope that Oracle officially still supports maintenance at present, and multiple WebLogic Server versions such as 10.3.6.0, 11.1.1.9 and 12.1.3.0 have stopped maintenance;

1. Vulnerability detection
	1. Local detection

You can run the following command to check whether the WebLogic version and patch have been installed.

|  |
| --- |
| $ cd /Oracle/Middleware/wlserver\_10.3/server/lib$ java -cp weblogic.jar   weblogic.version |

If no patch installation information is displayed in the output, a risk exists, as shown in the following figure.



* 1. T3 protocol detection

The Nmap tool provides a scanning script for the WebLogic T3 protocol to detect WebLogic hosts that enable the T3 service. The command is as follows:

|  |
| --- |
| nmap -n -v -Pn –sV [host or network segment address] -p7001,7002 --script=weblogic-t3-info.nse |

As shown in the red box of the following figure, the target has enabled T3 protocol and WebLogic version is within the affected range. If relevant personnel do not install official security patches, there will be a vulnerability risk.



* 1. Product testing

NSFOCUS Remote Security Assessment System (RSAS), Network Intrusion Detection System (IDS) and Integrated Threat Sensor (UTS) have the ability to scan and detect this vulnerability. Users who deploy these devices are requested to upgrade to the latest version.

|  |  |  |
| --- | --- | --- |
|  | **Version number of upgrade package** | **Upgrade package download link** |
| **RSAS V6 system plug-in package** | V6.0R02F01.3802 | https://update.nsfocus.com/update/listRsasDetail/v/vulsys |
| **IDS** | 5.6.11.37159 | https://update.nsfocus.com/update/listNewidsDetail/v/rule5.6.11 |
| **UTS** | 5.6.10.37159 | [https://update.nsfocus.com/update/listBsaUtsDetail/v/rule2.0.0](https://update.nsfocus.com/update/listBsaUtsDetail/v/rule2.0.0%22%20%5Ct%20%22_blank) |
| 2.0.0.37160 | [https://update.nsfocus.com/update/listBsaUtsDetail/v/rule2.0.1](https://update.nsfocus.com/update/listBsaUtsDetail/v/rule2.0.1%22%20%5Ct%20%22_blank) |
|  |  |  |

For RSAS upgrade configuration guidance, please refer to the following link:

https://mp.weixin.qq.com/s/SgOaCZeKrNn-4uR8Yj\_C3Q

1. Vulnerability protection
	1. Patch update

At present, the Oracle database has released patches to fix the above vulnerabilities. Please refer to the official notice to download the update patch of the affected product in time, and install the update by referring to the readme file in the patch installation package to ensure long-term effective protection.

Note: The official patch of Oracle requires the user to have a license account of genuine software. After logging in https://support.oracle.com with this account, you can download the latest patch.

* 1. Product protection

For this vulnerability, NSFOCUS Intrusion Prevention System (IPS) and Next-Generation Firewall (NF) have released a rule upgrade package. Please update the rule package to the latest version to form security product protection capabilities. The version number of the rules for security protection products is as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Safety protection products** | **Rule version number** | **Upgrade package download link** | **Rule No.** |
| **IPS** | 5.6.11.37159 | [https://update.nsfocus.com/update/listNewipsDetail/v/rule5.6.11](https://update.nsfocus.com/update/listNewipsDetail/v/rule5.6.11%22%20%5Ct%20%22_blank) | [28210] |
| 2.0.0.37160 | [https://update.nsfocus.com/update/listNewipsDetail/v/rule5.6.11\_v2](https://update.nsfocus.com/update/listNewipsDetail/v/rule5.6.11_v2%22%20%5Ct%20%22_blank) |
| **NF** | 2.0.0.37160 | [https://update.nsfocus.com/update/listNewNfDetail/v/rule6.0.5](https://update.nsfocus.com/update/listNewNfDetail/v/rule6.0.5%22%20%5Ct%20%22_blank) | [28210] |

Please refer to the following link for detailed operation steps of product rule upgrade:

IPS: https://mp.weixin.qq.com/s/DxQ3aaap8aujqZf-3VbNJg

NF: https://mp.weixin.qq.com/s/R3k\_KJm4O52bxy794jjo4A

* 1. Temporary protective measures

If users cannot install the update patch temporarily, you can take the following measures to temporarily protect high-risk vulnerabilities.

4.2.1 Restriction of T3 Protocol Access

Users can temporarily block attacks that exploit T3 protocol vulnerabilities by controlling access to the T3 protocol. WebLogic Server provides a default connection filter named weblogic.security.net.ConnectionFilterImpl, which accepts all incoming connections and can control access to T3 and T3s protocols through the configuration rules of this connection filter. The detailed operation steps are as follows:

1. Go to the WebLogic console. On the configuration page of base\_domain, go to the "Security" tab page and click "Filters" to configure connection filters.



2. Enter weblogic.security.net.ConnectionFilterImpl in the connection filter, and configure rules conforming to actual situation of enterprise in the connection filter rule by referring to the following writing:

|  |
| --- |
| 127.0.0.1 \* \* allow t3 t3sLocal IP \*\*allow t3 t3sIP allowed to be accessed \*\* allow t3 t3s\* \* \* deny t3 t3s |



|  |
| --- |
| The connection filter rule format is as follows: target localAddress localPort action protocols, where:* target specifies one or more servers to filter.
* localAddress defines the host address of the server. (If specified as an asterisk (\*), the returned match will be all local IP addresses.)
* localPort defines the port on which the server is listening. (If an asterisk is specified, the match will return all available ports on the server).
* action specifies the operation to be performed. (Value must be "allow" or "deny".)
* Protocols is a list of protocol names to be matched. (Must specify one of the following protocols: http, https, t3, t3s, giop, giops, dcom or ftp. ) If no protocol is defined, all protocols will be matched to one rule.
 |

3. If the rule does not take effect after saving, it is recommended to restart the WebLogic service (restarting the WebLogic service will cause business interruption. It is recommended that relevant personnel assess the risk before proceeding). Take the Windows environment as an example. The steps to restart the service are as follows:

Enter the bin directory under the directory where the domain is located, run stopWebLogic.cmd file in Windows system to terminate WebLogic service, and run stopWebLogic.sh file in Linux system.



After the termination script is executed, run the startWebLogic.cmd or startWebLogic.sh file to start WebLogic to restart the WebLogic service.

4.2.2 Disable IIOP Protocol

Users can block attacks that exploit IIOP protocol vulnerabilities by disabling the IIOP protocol. The operation is as follows:

In the WebLogic console, choose Service -> AdminServer -> Protocol and unselect Enable IIOP. Restart the WebLogic project to make the configuration take effect.



Representation

This security bulletin only describes possible security issues, and NSFOCUS does not provide any guarantee or commitment for this security bulletin. Any direct or indirect consequences and losses caused by the dissemination and use of the information provided in this safety bulletin shall be borne by the user himself/herself, while NSFOCUS and the authors of the safety bulletin do not assume any responsibility for this.

NSFOCUS reserves the right to modify and interpret this security bulletin. If you wish to reprint or distribute this security bulletin, you must ensure the integrity of this security bulletin, including the copyright notice in full. Without the permission of NSFOCUS, you are not allowed to arbitrarily modify or add/delete this safety bulletin or use it for commercial purposes in any way.