Web Application Firewall

Product Notices

Issue	01
Date	2022-05-12

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Java Spring Framework Remote Code Execution Vulnerability

Spring Framework is a lightweight open-source application framework for developing enterprise Java applications. A remote code execution (RCE) vulnerability was disclosed in the Spring framework and classified as critical. This vulnerability can be exploited to attack Java applications running on JDK 9 or later versions.

Vulnerability Name

Zero-Day RCE Vulnerability in the Spring Framework

Affected Versions

- JDK 9 or later
- Applications developed using the Spring Framework or derived framework

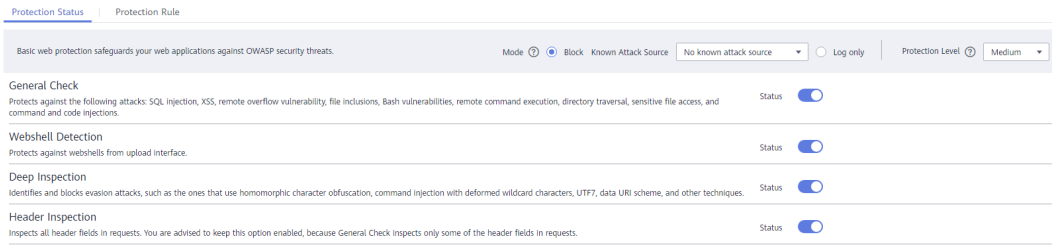
Mitigation

Step 1 **Buy WAF**.

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see **Adding a Domain Name to WAF**.

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Configuring Basic Web Protection Rules**.

Figure 1-1 Basic Web Protection



NOTICE

There are two types of malicious payload in this vulnerability. Whether to enable **Header Inspection** depends on the type of payloads in your services.

- Type 1: Malicious payloads are included in submitted parameters. In this situation, **Header Inspection** can be disabled.
- Type 2: Malicious payloads are included in a custom header field. In this situation, **Header Inspection** must be enabled to block attacks.

Type 2 malicious payloads depend on Type 1 malicious payloads so whether to enable **Header Inspection** is determined by your service requirements.

----End

2 Apache Dubbo Deserialization Vulnerability

On February 10, 2020, Apache Dubbo officially released the CVE-2019-17564 vulnerability notice, and the vulnerability severity is medium. Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. Now, Huawei Cloud WAF provides protection against this vulnerability.

Affected Versions

This vulnerability affects Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.*x*. versions.

Mitigation Version

Apache Dubbo 2.7.5

Solutions

Upgrade Apache Dubbo to version 2.7.5.

If a quick upgrade is not possible or you want to defend against more vulnerabilities, use Huawei Cloud WAF. The procedure is as follows:

Step 1 **Buy WAF**.

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see **Adding a Domain Name**.

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Configuring Basic Web Protection Rules**.

----End

3 DoS Vulnerability in the Open-Source Component Fastjson

On September 3, 2019, the Huawei Cloud security team detected a DoS vulnerability in multiple versions of the widely used open-source component Fastjson. An attacker can exploit this vulnerability to construct malicious requests and send them to the server that uses Fastjson. As a result, the memory and CPU of the server are used up, and the server breaks down, causing service breakdown. Huawei Cloud WAF provides protection against this vulnerability.

Affected Versions

Versions earlier than Fastjson 1.2.60

Mitigation Version

Fastjson 1.2.60

Official Solution

Upgrade the open-source component Fastjson to 1.2.60.

Mitigation

WAF can detect and defend against this vulnerability. The procedure is as follows:

Step 1 **Buy WAF**.

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see **Adding a Domain Name**.

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Enabling Basic Web Protection**.

----End

4 Remote Code Execution Vulnerability of Fastjson

On July 12, 2019, the Huawei Cloud Emergency Response Center detected that the open-source component Fastjson had a remote code execution vulnerability. This vulnerability is an extension of the deserialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.

Affected Versions

Versions earlier than Fastjson 1.2.51

Mitigation Version

Fastjson 1.2.51 or later

Official Solution

Upgrade Fastjson to 1.2.51 or the latest 1.2.58 version.

Mitigation

The built-in protection rules of Huawei Cloud WAF can defend against this vulnerability. The procedure is as follows:

Step 1 **Buy WAF**.

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see **Adding a Domain Name**.

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Enabling Basic Web Protection**.

----End

5 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)

On April 17, 2019, Huawei Cloud Emergency Response Center found that China's National Vulnerability Database (CNVD) released a security notice on Oracle WebLogic wls9-async component. It revealed that the component had a deserialization vulnerability. Unauthorized remote attackers can use this vulnerability to implement remote code execution and gain server permissions.

Vulnerability ID

CNVD-C-2019-48814

Vulnerability Name

Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability

Vulnerability Description

The WebLogic wls9-async component has a defect. The website built on the WebLogic Server has security risks. Attackers can construct HTTP requests to obtain the permission of the target server and execute arbitrary code remotely without authorization.

Affected Products

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

Official Solution

The patch for fixing this vulnerability has not been released.

Mitigation

Configure precise protection rules to restrict access from the URLs whose prefixes are **/_async/** or **/wls-wsat/** by referring to **Figure 5-1** and **Figure 5-2** and block remote code execution requests initiated by exploiting this vulnerability. For details, see **Configuring a Precise Protection Rule**.

Figure 5-1 async configuration

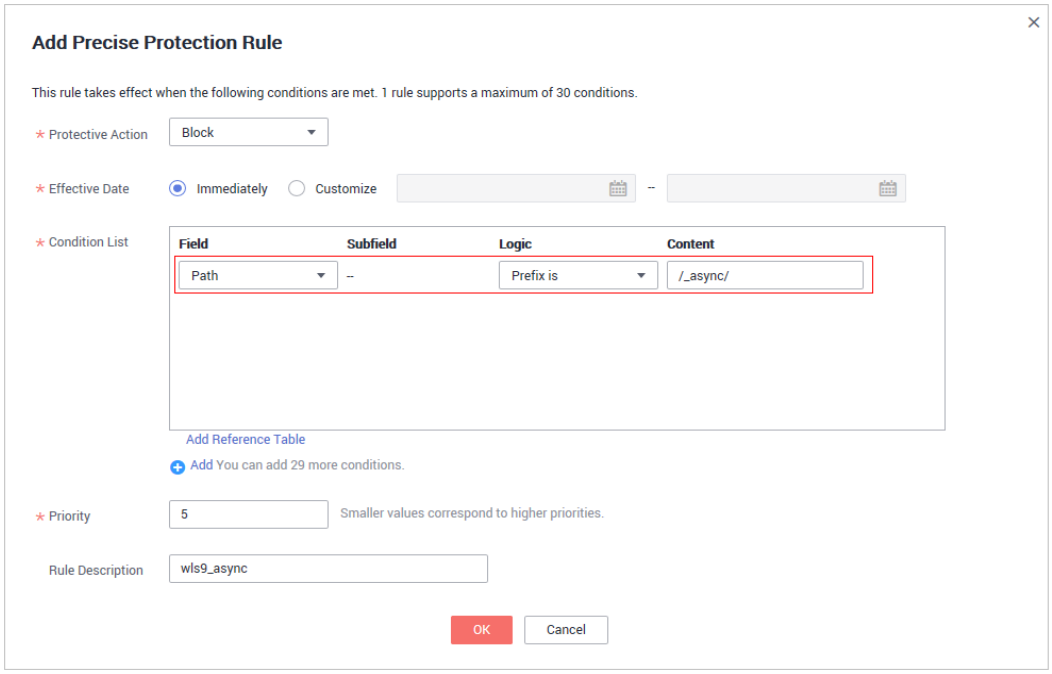


Figure 5-2 wls-wsat configuration