ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Announcements & Updates

Document Version: 20201021

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Protection engine upgrade

From March 11, 2020, Web Application Firewall (WAF) upgraded the protection engine for all users. The new protection engine is reliable and easy to use.

The new protection engine offers the following benefits:

- Improved protection effects

  Functions are integrated into protection modules, such as web intrusion prevention, data security, bot management, and access control and throttling. The modules provide protection for your business.

  The new protection engine also provides precise throttling and account security capabilities. These capabilities allow you to protect your servers from unauthorized access, HTTP flood attacks, credential stuffing, weak password attacks, and brute-force attacks. After the upgrade, WAF displays a visual report of the security and protection services.

- Fine-grained throttling can be achieved by using custom protection policies.

  The custom protection policy feature allows you to configure more fields and rules. It also provides you with precise throttling capabilities under complex conditions. This feature enables you to manage unauthorized access requests in various business scenarios.

  - The custom HTTP flood protection rules in the original engine are integrated into custom protection policies to provide more precise throttling capabilities. For more information, see Create a custom protection policy.
  - The original HTTP ACL policy feature can be used to allow legitimate traffic. After the upgrade, you can configure website whitelists for each protection module to allow legitimate traffic. For more information, see Configure the website whitelist.

- Convenient IP address blacklist configuration

  You can add IP addresses, CIDR blocks, and the regions to which IP addresses belong to blacklists. This way, you can implement quick access control and block traffic.

You can configure the following items for each protection module: website whitelists, scan reports, and priorities of protection rules. For more information, see Configure RegEx Protection Engine.

Upgrade your protection engine

The protection engine will be upgraded for all users who activated WAF before January 2020. After the engine is upgraded in the backend, you will receive an upgrade notification when you log on to the WAF console. Then, you can click **Try Now** to experience your new protection engine.

2.Release notes

This topic describes the release notes for Web Application Firewall (WAF) features.

2020

Release date	Feature update	Description	Documentation
2020-06-08	API security released	The API security module is added to WAF. This module is suitable for users whose websites provide API services. You can formulate API conventions to protect against malicious API requests. This protects website assets from data tampering and replay attacks.	Enable API request security
2020-06-04	Custom protection rule groups and Overview page optimized	• Rules in custom rule groups can be automatically updated, which improves security and availability of the groups. • The protection rule details and impact scopes of zero-day vulnerabilities are displayed on the Overview page.	Customize protection rule groups View overall information
2020-05-20	Big Data Deep Learning Engine optimized	Attack probability thresholds are adjustable to achieve optimal protection effects for different businesses.	Configure the Big Data Deep Learning Engine
2020-05-18	Support for Terraform	Terraform is supported to suit O&M needs of large enterprises. It allows you to perform basic operations, such as managing domain names and policies, by using code. ? **Note** This feature also enables automated operations in the console, achieving high operational efficiencies and eliminating human errors. For more information, see Terraform documentation.	None

Release date	Feature update	Description	Documentation
2020-04-10	User experience optimized	Data on the Overview page can now be drilled down to the Security report page. Data on the Security report page can be drilled down to the Log Service page, which closes the loop of operations data. • Data in the Protection statistics area of the **Overview** page can be drilled down to the Security report page. The ranking on the **URL Requests** tab shows domain name information. • Statistics on the **Access Control/Throttling** tab of the **Security report** page can be drilled down to the Log Service page. Custom access control rules that match access requests can be viewed and edited.	View overall information View security reports
2020-04-02	Support for bot management	Value-added services such as bot management and application protection are supported to provide intelligent protection against automated attacks and intelligent protection of bot traffic. The bot management module provides trusted communications to protect native applications and defends against bot script abuse. **Note** The bot management and application protection modules are available only to the new protection engine released in January 2020. If you are using a protection engine of an earlier version, we recommend that you upgrade your protection engine at the earliest opportunity.	Configure the bot management whitelist Overview
2020-03-10	Upgrade guide released for the new protection engine	An upgrade guide is provided to instruct existing users to upgrade their protection engines without service interruption.	Protection engine upgrade

Release date	Feature update	Description	Documentation
2020-03-04	Support for intelligent load balancing among multiple SLB service nodes	Intelligent load balancing is supported. WAF connects to multiple SLB service nodes to enable automatic disaster recovery and optimal routing with low latency.	Intelligent load balancing
2020-02-14	Log Service for WAF upgraded and user experience optimized	Log Service for WAF is upgraded. You can customize domain names to enable features such as full log service.	None
2020-02-10	Event alert feature upgraded	The alert notification feature is upgraded to provide basic statistics and details about security events and workload monitoring. Related alerts are provided to support routine O&M.	Configure alert rules
2020-01-15	Protection capabilities and user experience upgraded	Fine-grained throttling and robust protection against malicious network traffic are supported in the new protection engine of WAF. The account security feature can be enabled to protect against common HTTP flood attacks, credential stuffing, and weak password sniffing. **Note** The protection capabilities work for all users but can be directly enabled only by users who newly purchased WAF instances in the console. Existing users must wait until March 2020 before they can upgrade their WAF instances to enable the protection capabilities.	Configure the RegEx Protection Engine

2019

Release date	Feature update	Description	Documentation
2019-12-20	Features in the Exclusive edition optimized	Features in the WAF Exclusive edition are optimized. You can customize the request timeout period for your domain name.	Create an exclusive cluster

Release date	Feature update	Description	Documentation
2019-11-28	Support for account security detection	The account security feature allows you to detect account security risks on logon interfaces. The risks include credential stuffing, brute-force attacks, zombie accounts, weak password sniffing, and SMS interface abuse.	Configure account security
2019-10-25	Exclusive edition released	The WAF Exclusive edition is released. It allows you to customize items such as protection ports, TLS versions, cipher suites, and the response page that appears when a request is blocked. This edition meets your special requirements for web application protection.	Create an exclusive cluster
2019-10-22	URL profiling supported for protected websites	URL profiling is supported. WAF can automatically identify business URL profiles and business volumes based on the normal network traffic that flowed through websites. This allows you to customize protection policies for different websites.	None
2019-10-16	Data of website scanning protection provided on the Overview page	The volume of traffic blocked by the anti-scanning module, a list of blocked website scanning attacks, attack details, and resolutions provided by security experts are displayed on the Overview page in the WAF console.	View overall information
2019-08-22	Positive security model released	Based on algorithms for intelligent big data learning, the positive security model learns historical network traffic of users in an iterative manner. This allows you to customize automatic protection policies.	Configure the positive security model
2019-07-18	Web attack details added to the Security report page	Web attack details are added to the Security report page to show the specific causes of blocked attacks. This improves the efficiency of security O&M.	View security reports
2019-06-27	Support for HTTP/2-compliant application protection	HTTP/2-compliant application protection is supported. It increases the coverage rate of application protocols. This ensures that the applications of WAF users are fully protected.	Add domain names

Release date	Feature update	Description	Documentation
2019-06-13	Support for decoding methods of web request content in protection configuration	Decoding methods of web request content can be customized in protection configuration.	Configure the RegEx Protection Engine
2019-05-30	ACL rules optimized	Multiple IP addresses or CIDR blocks can be added to ACL rules for condition matching.	Create a custom protection policy
2019-05-30	Overview page optimized	The Overview page in the WAF console is optimized. On this page, the system aggregates security operations events based on a large volume of log data and provides professional suggestions for event handling. This page also displays the number of attacks by type and the frequently attacked domain names. After the optimization, the operations capabilities of WAF are enhanced.	View overall information
2019-03-19	Threat intelligence feature released	The threat intelligence feature is released. It provides a library that contains scanning attack information. Based on the provided information, you can customize the thresholds of network scanning frequency and duration for blocking malicious scanning attacks. This feature is used to prevent scanning attacks with common signatures, such as path traversal.	Configure scan protection
2019-01-03	Custom country or region supported for request blocking	All requests from the IP addresses in the blocked countries or regions are denied by WAF.	Configure a blacklist

2018

Release date	Feature update	Description	Documentation
2018-12-20	Website defacement-prevention API operations released	Website defacement-prevention API operations are released. You can call these operations to update cached pages and add protection rules.	None

Release date	Feature update	Description	Documentation
2018-12-13	Support for customization of protection rule groups for web applications	Protection rule groups for web applications can be customized, so you can configure rules based on your business requirements. This prevents false request blocking caused by default protection rules and ensures business security.	Customize protection rule groups
2018-11-16	Support for one-year storage of business logs	WAF is integrated with Log Service to collect, query, and analyze business logs of websites that are added to WAF in real time.	Use full logs
2018-10-24	Support for traffic marking	Traffic marking is supported. You can specify a header field name and value to mark the traffic forwarded by WAF.	Add domain names
2018-10-17	Support for query of blocking events in all logs by using a unique ID	A unique ID can be used to query blocking events in all logs, so you can locate the cause of request blocking and view the request details.	Use full logs
2018-10-01	Support for security events and alerts	Security events and system alerts can be sent to you by using text messages or emails. You can customize metrics to detect business exceptions in a timely manner.	Configure alert rules
2018-08-09	Support for the Big Data Deep Learning Engine	The Big Data Deep Learning Engine is supported. It offers powerful machine learning capabilities for WAF to identify exceptions and block risky requests.	Configure the Big Data Deep Learning Engine
2018-07-27	API operations provided	API operations for common configurations in the console are provided to facilitate batch processing.	API overview
2018-04-27	Precise access control enhanced	More HTTP header fields can be used to set ACL rules and filter access requests.	Create a custom protection policy
2018-03-15	Support for release of WAF instances	WAF instances can be released in the console based on business requirements.	Release WAF instance
2018-01-30	Support for download of all logs	In Business or higher editions, intelligent searches across all access logs are supported, and download of log search results with a few clicks is implemented.	Use full logs

2017

Release date	Feature update	Description
2017-12-28	Non-standard ports added	More non-standard ports are supported for protection.
2017-11-24	Support for multiple load balancing algorithms	Multiple load balancing algorithms can be selected as required to meet different business requirements.
2017-10-30	Application security solutions provided	Application security solutions are provided to protect your applications from traffic flooding attacks and data crawling.
2017-10-26	Support for WebSocket	WebSocket-compliant website business is supported.
2017-08-31	Support for monitoring of error codes	Error codes can be monitored.
2017-08-31	Support for query of business bandwidth	The uplink and downlink bandwidth usage of business can be queried.
2017-08-31	Support for business QPS	The QPS by instance or domain name is supported.
2017-08-16	Support for viewing details of blackhole events	The information such as attack thresholds and events generated when a blackhole occurs can be viewed.
2017-07-27	Exclusive WAF IP addresses released	Exclusive WAF IP addresses are released. You can purchase exclusive WAF IP addresses to protect specified domain names.
2017-07-25	Precise access control optimized	Policies for risk control on allowed access requests and region blocking can be configured in precise access control rules.
2017-07-25	CAPTCHA algorithm optimized	The CAPTCHA algorithm in custom HTTP flood protection rules is optimized, which improves the accuracy in blocking HTTP flood attacks.
2017-07-25	Support for more logical operators	Logical operators such as "Does not exist" and "Value length range" are added to define precise access control rules.

Release date	Feature update	Description
2017-07-25	Support for detection of more HTTP fields	Rules for detection of more HTTP fields are supported in precise access control.
2017-06-07	Support for the back-to-origin CIDR block feature	Back-to-origin addresses can be set to domain names in website configuration.
2017-05-25	Data leakage prevention feature released	A sensitive data leakage prevention scheme is released based on network security regulations.
2017-04-12	HTTPS implementation with a few clicks	HTTPS-based website access is implemented with a few clicks, without changes in server configurations.
2017-04-12	Support for non-standard ports in multiple editions of WAF	Non-standard ports are supported in multiple editions of WAF for security protection.
2017-03-28	Support for the big-data threat intelligence feature	The big-data threat intelligence feature is supported. Services such as security check score assessment, high-risk warning, and viewing of hacking tools are provided.
2017-03-08	Access experience optimized	DNS records can be added with a few clicks.
2017-02-09	Support for the website defacement-prevention feature	The website defacement-prevention feature is supported to protect web page data from being tampered with.
2017-02-09	Log search feature released	All of the service access logs can be searched with a few clicks.
2017-01-05	Support for virtual hosts	Virtual hosts (HiChina) are supported for website security protection.

2016

Release date	Feature update	Description
2016-12-21	WAF V3.1 released	WAF V3.1 is released. It improves the core protection capabilities of protection engines and provides features such as blocking IP addresses from specified regions and customizing protection rules to block HTTP flood attacks.

Release date	Feature update	Description
2016-12-01	Intelligent Semantic Analysis Engine provided	The Intelligent Semantic Analysis Engine is provided. Compared with the RegEx Protection Engine, this engine reduces false positives.

3.Security bulletin

3.1. Fastjson zero-day RCE vulnerability detected on July 23, 2019

On July 23, 2019, Alibaba Cloud Security emergency response center discovered a zero-day remote code execution (RCE) vulnerability in Fastjson. Attackers can exploit the vulnerability and bypass blacklist policies to execute malicious code.

Vulnerability name

Fastjson zero-day RCE vulnerability

Vulnerability description

Attackers can exploit the zero-day vulnerability to craft a request and bypass Fastjson blacklist policies to execute malicious code. For example, an attacker can craft a request and remotely execute specified commands on a server. In this example, a calculator program is running.

Affected versions

- Fastjson 1.2.24 and earlier
- Fastjson 1.2.41 to 1.2.45

Solution

Upgrade Fastjson to the latest version. We recommend that you upgrade Fastjson to 1.2.58.

> **Note** We recommend that you also upgrade Fastjson outside the affected versions.

Upgrade method

You can update Maven dependency configurations to upgrade Fastjson to 1.2.58.

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

Protection recommendations

By default, WAF protects against the zero-day vulnerability in Fastjson. You only need to enable the protection function.

3.2. Fastjson zero-day RCE vulnerability detected on June 22, 2019

On June 22, 2019, Alibaba Cloud Security emergency response center discovered a zero-day remote code execution (RCE) vulnerability in Fastjson. Attackers can exploit the vulnerability and bypass blacklist policies to execute malicious code.

Vulnerability name

Fastjson zero-day RCE vulnerability

Vulnerability description

Attackers can exploit the zero-day vulnerability to craft a request and bypass Fastjson blacklist policies to execute malicious code. For example, an attacker can craft a request and remotely execute specified commands on a server. In this example, a calculator program is running.

Affected versions

Fastjson versions earlier than 1.2.48

Solution

Upgrade Fastjson to the latest version. We recommend that you upgrade Fastjson to 1.2.58.

> Note We recommend that you also upgrade Fastjson outside the affected versions.

Upgrade method

You can update Maven dependency configurations to upgrade Fastjson to 1.2.58.

```
<dependency>
 <groupId>com.alibaba</groupId>
 <artifactId>fastjson</artifactId>
 <version>1.2.58</version>
</dependency>
```

Protection recommendations

By default, WAF protects against the zero-day vulnerability in Fastjson. You only need to enable the protection function.

> Note If you use custom protection rules, you must add the following rule to a custom rule group. For more information, see Customize protection rule groups.

3.3. RCE vulnerability in Consul service APIs

On November 27, 2018, Consul released a vulnerability notice on its official blog. The notice stated that a remote code execution (RCE) vulnerability might be caused by Consul with specific configurations, and outlined a solution to fix this vulnerability.

Consul is an open source tool developed by HashiCorp. This tool is used to discover and configure services in distributed systems and provides an end-to-end solution. Consul provides multiple features, such as service registration and discovery, consensus protocol implementation, health checking, key-value store, and multi-data center support. All this makes Consul simple to configure and independent of other tools, such as ZooKeeper.

Consul is written in Go and supports Linux, Windows, and Mac OS X. Therefore, it is portable. Consul is easy to deploy because its installation package contains only one executable file. Consul works well together with lightweight containers such as Docker.

Vulnerability name

RCE vulnerability in HashiCorp Consul service APIs

Vulnerability description

Attackers can send crafted HTTP requests and remotely execute commands without authorization on Consul servers that have specific configurations. For more information about the Consul vulnerability, see Protecting Consul from RCE Risk in Specific Configurations.

Reproduce the vulnerability

1. Verify whether your Consul server is exposed to the RCE vulnerability.

2. Craft an HTTP PUT request and remotely execute commands on the Consul server.

Affected versions

All versions of Consul in which -enable-script-checks is set to true to enable the script check function

Protection recommendations

To protect against this vulnerability, you can use one of the following solutions:

- Disable the script check function on the Consul server.
- If you need to use the script check function of Consul, upgrade Consul to one of the following versions: 0.9.4, 1.0.8, 1.1.1, or 1.2.4. This changes -enable-script-checks to -enable-local-script-checks. These versions of Consul support the -enable-local-script-checks parameter.
- Make sure that you cannot call or access Consul HTTP APIs over the Internet.
- Enable the custom protection policy feature of WAF and configure the protection rule shown in the following figure. This rule blocks requests that use the HTTP PUT method and contain `/v1/agent/service/register` in their URLs. For more information, see Create a custom protection policy.

3.4. Apache Solr deserialization RCE vulnerability (CVE-2019-0192)

On March 7, 2019, Alibaba Cloud Security emergency response center detected a Solr security bulletin issued by Apache. Attackers can call the Config API and modify the jmx.serviceUrl attribute to point to a malicious RMI service, which causes a deserialization remote code execution (RCE) vulnerability in Apache Solr.

CVE ID

CVE-2019-0192

Vulnerability name

Deserialization RCE vulnerability in Apache Solr

Vulnerability description

The Config API allows to configure the jmx.serviceUrl attribute by using an HTTP POST request. This configuration modifies the Apache Solr JMX server. Attackers can point the request to a malicious RMI server and take advantage of the unsafe deserialization of Solr to trigger RCE.

Affected versions

- Apache Solr 5.00 to 5.5.5
- Apache Solr 6.00 to v6.6.5

Solution

- Upgrade your Apache Solr to 7.0 or later.
- Disable the Config API by configuring `disable.configEdit=true` .
- Ensure that only trusted traffic is allowed to access the Solr server at the network layer.

If you cannot resolve the issue by using the first two solutions, recompile Solr by using the official patch.

Protection recommendations

If you do not want to upgrade Solr to resolve this vulnerability, we recommend that you use the custom protection policy feature provided by WAF to protect your business.

You can use the custom protection policy feature to restrict POST requests that contain specific JSON data, such as service:jmx:rmi. This can also prevent RCE attacks.

3.5. Arbitrary file read vulnerability in Jenkins (CVE-2018-1999002)

On July 18, 2018, Jenkins released its latest security bulletin and announced multiple security vulnerabilities. SECURITY-914 is an arbitrary file read vulnerability reported by Orange.

Attackers can exploit this critical vulnerability to read arbitrary files on Windows servers and, under specific conditions, read files on Linux servers. Attackers can also obtain credential information in Jenkins systems and therefore expose sensitive user information. Some credentials may be user passwords, which enable the attackers to log on to the Jenkins systems and execute commands.

CVE ID

CVE-2018-1999002

Vulnerability name

Arbitrary file read vulnerability in Jenkins

Vulnerability description

An arbitrary file read vulnerability in the Stapler web framework used by Jenkins allows unauthenticated users to send crafted HTTP requests. The requests return the contents of any file on the Jenkins master file system that is accessible by the Jenkins master process.

For more information about this vulnerability, visit Jenkins security advisory.

Affected versions

- Jenkins weekly 2.132 and earlier
- Jenkins LTS 2.121.1 and earlier

Solution

- Upgrade Jenkins weekly to 2.133.
- Upgrade Jenkins LTS to 2.121.2.

Protection recommendations

If you do not want to upgrade Jenkins to fix this vulnerability, we recommend that you use the custom protection policy feature provided by WAF to protect your business.

You can use this feature to create a rule that blocks requests whose header field Accept-Language contains `... /` . This prevents attackers from exploiting this vulnerability to read arbitrary files by using directory traversal.

Protective effects

Based on the custom protection policy, WAF blocks the HTTP request that attempts to exploit the vulnerability.

> **Note** For more information about the custom protection policy feature, see Custom protection policy.

3.6. DoS vulnerability in the Apache Struts2 REST plug-in (CVE-2018-1327)

Two security experts (Yevgeniy Grushka and Alvaro Munoz) from Hewlett Packard Enterprise (HPE) found a denial of service (DoS) vulnerability in the Apache Struts2 REST plug-in. If you use the XStream library in the Struts REST plug-in, an attacker can construct a malicious XML request to launch a DoS attack.

CVE ID

CVE-2018-1327

Vulnerability name

DoS vulnerability in the Apache Struts2 REST plug-in (S2-056)

Vulnerability description

The S2-056 vulnerability exists in the Apache Struts2 REST plug-in. If you use the XStream library to deserialize a packet in the XML format and the data content is not validated, attackers can launch remote DoS attacks by sending malicious XML data.

If attackers initiate large amounts of attack requests, the CPU resources of the server where your applications reside will be used up rapidly.

For more information about the vulnerability, visit Official vulnerability disclosure.

Affected versions

Struts 2.1.1 to 2.5.14.1

Solution

Upgrade your Apache Struts to 2.5.16.

Protection recommendations

If you do not want to upgrade Apache Struts to fix the vulnerability, we recommend that you use the custom protection policy and HTTP flood protection features provided by WAF to protect your business.

- You can use the custom protection policy feature to create a rule. The rule blocks the POST requests that contain specific XML data (`com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource`). This prevents the DoS attack requests launched by using this vulnerability. For example, configure the following rule to block attack requests to applications that use Apache Struts whose REST plug-in uses the XStream library.
- You can use the HTTP flood protection feature to limit the frequency of requests from an IP address, for example, requests to applications that use Apache Struts whose REST plug-in uses the XStream library. For example, configure the following rule to make sure that the request frequency to a specified page does not exceed 100 times every 5 seconds.

For more information about the custom protection policy and HTTP flood protection features, see Custom protection policy and HTTP flood protection.

3.7. WordPress DoS vulnerability (CVE-2018-6389)

On February 5, 2018, a security researcher disclosed a denial-of-service (DoS) vulnerability in WordPress. The vulnerability affects all versions of WordPress from 3.x to 4.x. Attackers can trigger a DoS attack and consume server resources by using WordPress to load multiple JavaScript files in a single request.

WAF is not affected by this vulnerability. However, if your website business uses WordPress, we recommend that you configure appropriate protection rules.

Vulnerability description

This vulnerability is found in the *load-scripts.php* file. *load-scripts.php* is the built-in script of WordPress, a Content Management System (CMS) system. The *load-scripts.php* file selectively calls required JavaScript files by passing their `names` into the `load` parameter. The `names` are separated with commas (,).

For example, in the request of `https://example.com/wp-admin/load-scripts.php?c=1&load[]=jquery-ui-core,editor&ver=4.9.1` , JavaScript files *jquery-ui-core* and *editor* are loaded.

All 181 JavaScript files defined in the *script-loader.php* file can be loaded in a single request. An attacker can send a large number of requests without authorization, and this results in increased server load and triggers DoS attacks.

Protection recommendations

We recommend that you use the custom protection policy and HTTP flood protection features provided by WAF to protect your WordPress website.

- You can use the custom protection policy feature to restrict the number of parameters passed by *load-scripts.php*. For example, you can add the following rule to restrict the length of the parameter passed by *load-scripts.php* to up to 50 characters.
- You can also use the custom HTTP flood protection feature to restrict the frequency at which IP addresses can send requests to the *load-scripts.php* file. For example, you can add the following rule to restrict the frequency at which an IP address sends requests to the *load-scripts.php* file to up to 100 times per 5 seconds.

For more information about the custom protection policy and custom HTTP flood protection features, see Custom protection policy and HTTP flood protection.

3.8. WordPress XML-RPC pingback attacks

This topic describes how to prevent WordPress pingback attacks by using WAF.

Introduction to WordPress pingback attacks

WordPress is a blog platform that is written in PHP, and a pingback is a plug-in of WordPress. Attackers can use the pingback to initiate WordPress pingback attacks against a website.

When WordPress pingback attacks occur, a large number of requests are displayed on the server log, and the User-Agent fields of these requests contain WordPress and pingback.

As a variant of HTTP flood attacks, WordPress pingback attacks typically cause the following problems: slow web page loading, high CPU utilization, and no response from servers.

Use WAF to defend against WordPress pingback attacks

1. Log on to the WAF console.
2. In the left-side navigation pane, choose **Protection Settings** > **Website Protection**.
3. Click the **Access Control/Throttling** tab.
4. In the **Custom Protection Policy** section, click **Settings**.
5. Click **Custom Protection Policy** and add the following two rules.
    - Block access requests that contain pingback in User-Agent.
        - **Rule name**: Enter wp1.
        - **Matching field**: Select User-Agent.
        - **Logical operator**: Select Includes.
        - **Matching content**: Enter pingback.
        - **Action**: Select block.
    - Block access requests that contain WordPress in User-Agent.
        - **Rule name**: Enter wp2.
        - **Matching field**: Select User-Agent.
        - **Logical operator**: Select Includes.
        - **Matching content**:Enter WordPress.
        - **Action**: Select block.

    > **Note** You must add the two rules separately.