Web Application Firewall

Release Notes and Announcements

Product Documentation

Contents

Release Notes and Announcements

Release Notes

Last updated：2024-08-28 20:10:35

July 2024

Update	Description	Release Date	Documentation
Access capability optimization	CLB-WAF supported configuring multiple domain name policies within CLB listeners, enabling full access to WAF protection for all domain names, thereby enhancing the overall access experience. The SaaS-WAF access experience had been optimized by ensuring that private IP addresses cannot be configured as origin-pull addresses and that there were detection and reminders for spaces entered in domain names.	2024-07-22	-
Basic security protection capability optimization	The security rule engine's rule database had been enhanced with a new risk level field, allowing for the filtering of rules based on different threat risk levels, thereby improving the efficiency of security operations. The security rule engine's rule database supported the fuzzy retrieval for the rule content description field, enhancing the customer experience in querying about protection rules for improved security operations. Field and matching methods in CC protection had been optimized, improving the user experience. The IP query capability had been optimized by enhancing ban query capabilities and adding IP ban log queries. The number of domain names supported for an effective single rule configuration in batch protection has been increased to 300, improving the batch protection experience.	2024-07-22	-
Mini programs' security acceleration feature optimization	Automatic access had been extended to support the developer edition and includes the ability to switch between the developer edition and trial edition, enhancing the user experience during the access testing process. Both automatic and manual access supported advanced configuration, allowing users to customize the capitalization	2024-07-22	-

	of the first letter in response packet header field names. Automatic access supported custom configuration of the grayscale release ratio for all editions, enhancing access stability and user experience. Manual access had been extended to support both WebSDK and AppSDK, effectively enabling full traffic access to the mini programs security acceleration gateway for comprehensive business protection.		
API security feature optimization	API security supported accessing more traffic logs for detection, allowing the shipping of response body traffic from domain names/objects accessed by CLB-WAF or traffic not accessed by WAF to WAF-provided CKafka for API asset discovery and security detection. API security rule configuration had been continuously optimized, allowing both API traffic throttling and API authentication features to support regular expression match or direct selection of discovered API assets, thereby enhancing the configuration flexibility. API security supported customizing the number of saved asset parameter samples with the ability to switch between them for viewing, as well as quickly copying the sample content. The API asset list supported custom policies for determining inactive APIs, enabling effective management of the API asset lifecycle.	2024-07-22	-

May 2024

Update	Description	Release Date	Documentation
Billing capability optimization	The mini programs security acceleration included an additional billing option for mini program nodes, supporting the expansion of the number of mini programs that can be accessed. This was designed to accommodate the needs of large-scale mini program businesses accessing the same WAF instance simultaneously. A new postpaid billing management page had been added, allowing users to view detailed historical elastic postpaid bills for easier bill detail queries. Newly purchased value-added and expansion capability resources supported automatic association with instance	2024-05-31	-

	tags. Security log packages were user-specific, allowing resource tags to be set for the log service package individually on the instance management page after purchase.		
Protection capability optimization	CC protection enhancements supported a threshold of 100,000 requests within a 5-minute interval, improving the protection capabilities of custom CC rules. CAPTCHA actions supported customizing exemption duration, penalty duration, and retry limits for each domain name.	2024-05-31	-
API security feature optimization	The API asset list included API authentication detection and display, as well as the ability to add API remarks. Additionally, a new asset hardening operation had been introduced, allowing one-click addition of input parameter detection and traffic throttling rules to the current API. API security included the ability to create custom feature scene tags, allowing batch assignment of these tags to APIs that match specific request characteristics through rule configuration. After API security was enabled on CLB-WAF, it supported detecting response traffic by shipping the traffic to WAF CKafka. The display of API event details in event management had been optimized by adding an attack source IP view, allowing for quick assessment of the impact and prompt action on the attack source.	2024-05-31	-
Log and monitoring optimization	The security overview included a Top 5 bandwidth statistics feature for proxy access traffic, helping customers identify high-bandwidth businesses and thereby enhancing the business operation experience. A new event alarm capability had been added, allowing for scheduled alarms for newly detected API and BOT events in event management. Notifications could be sent daily or hourly via internal messages and emails. Access log storage and shipping settings supported customizing options to include BOT information. When it was enabled, request records and shipped logs that hit the BOT module contained related BOT fields. The stability monitoring of SAAS-WAF service IP addresses supported integration with Tencent Cloud Observability Platform, allowing users to customize real-time monitoring and alarm services for WAF monitoring, thereby improving business operation efficiency.	2024-05-31	-

March 2024

Update	Description	Release Date	Documentation
Billing capability and specification optimization	WAF elastic billing supported bandwidth-based elastic billing, suitable for elastic protection of low QPS and high bandwidth businesses. The number of custom domain name policies and precise allowlist policy rules had been expanded to better support complex business security Ops. Mini programs security acceleration supported elastic billing, meeting the need for protection during sudden traffic spikes. Mini programs security acceleration supported an increased access number of mini program IDs. The Advanced Edition had been upgraded to support up to 3 mini program IDs, while the Enterprise and Ultimate Editions supported up to 4 mini program IDs.	2024-03-20	-
Mini programs security acceleration access capability optimization	Mini programs security acceleration supported access through cloud native gateways, APISIX, and custom hybrid cloud gateway domain names, enhancing coverage and optimizing the access experience. Automatic access supported API interface-based access, catering to the personalized needs of core business access. Manual access supported adding multiple origin server domain names and ports, meeting the needs for multi-domain name origin-pull requests.	2024-03-20	-
API security feature optimization	API security supported detecting horizontal privilege escalation and cross-border data transfer events. The API asset list supported grouping assets according to an asset tree, making the API asset hierarchy clearer.	2024-03-20	API Security
BOT protection capability optimization	The BOT expert rule set supported batch switching to redirection or CAPTCHA actions, providing more diverse protection options. The BOT expert rule set included protection level settings, allowing for switching between strict mode and normal mode.	2024-03-20	-
BOT event management	Event management capabilities supported BOT risk event alarms, one-click handling, and attack source analysis,	2024-03-20	-

capability release	enhancing the efficiency of BOT traffic protection and response.		
Protection configuration experience optimization	Custom rules and precise allowlists supported more matching methods, allowing for more flexible traffic matching.	2024-03-20	-
Log and monitoring capability optimization	Custom access log storage alarm thresholds could be set, with notifications triggered when the specified percentage was reached. Access logs had been enhanced with a richer set of fields and operators, improving the retrieval experience. Tencent Cloud Observability Platform supported QPS and bandwidth utilization metrics for Web Application Firewall, optimizing the monitoring experience.	2024-03-20	Access Log Settings
Access capability optimization	SAAS-WAF access domain names had been optimized to disable proxy caching, supporting the access of SSE protocol businesses. CLB-WAF provided visibility into the access status of domain names and objects, enhancing the access experience. The access list supported customizing column settings, meeting personalized domain name management needs and improving the user experience in access management.	2024-03-20	Domain Name Management

January 2024

Update	Description	Release Date	Documentation
API security feature optimization	API security asset list optimization The display of sensitive assets had been optimized, allowing for filtering and viewing of assets with sensitive data in the request body or response body. API parameter sample display had been optimized, now supporting the customization of parameter displays with generalized data. API security detection events had been enriched with the addition of monitoring for three types of events: vertical privilege escalation, unauthorized access to sensitive information, and excessive sensitive information retrieval. This enhanced the ability to discover API asset risks.	2024-01-22	API Security

	API security included authentication credential configuration: it supported setting up credential recognition rules for individual APIs or all APIs under a domain name. Custom rules were applied first, and if no custom rules were added, the system's built-in rules would be used for recognition.		
BOT management capability optimization	Session management capabilities in BOT management had been optimized: you could set different session identification extraction rules and prioritize them based on different protection scenes. The session identification parameters also supported extraction through parsing two layers of JSON. BOT custom rules supported more parameter configurations: added support for the number of sessions per IP, the most frequent COOKIE, and the most frequent UA fields, allowing for the configuration of related protection rules.	2024-01-22	Advanced BOT Management Settings
Access log shipping was supported for regions outside the Chinese mainland.	Log data could be shipped to CLS and TDMQ for CKafka, with billing based on the actual volume shipped.	2024-01-22	Log Shipping
Protection configuration experience optimization	Protection configuration rules supported IPV6 and IPV6 address range settings, enhancing the configuration experience. Access control rule parameters supported matching empty content values, enhancing traffic management capabilities. The Tiga engine supported adding multiple rule IDs to the allowlist for the same URL, improving the user experience. The batch protection feature supported adding IP blocking rules, allowing for the management of IP blocking rules across multiple domain names.	2024-01-22	Basic Security
Object access supported enabling BOT protection and API security protection.	Once this feature was enabled, it supported the quick activation of BOT management and API security analysis and protection for CLB objects.	2024-01-22	-

Access list optimization	Optimized domain name access status display: SaaS-based WAF offered detailed prompts for certificate and DNS resolution status of accessed domain names, along with guidance for resolving abnormal statuses. The SaaS-based WAF supported custom WebSocket timeout settings, custom origin-pull HOST settings, and the addition of custom remarks for accessed domain names. Object access supported custom Layer-7 proxy services: once enabled, the client IP determination method could be set.	2024-01-22	Domain Name Management

December 2023

Update	Description	Release Date	Documentation
Mini programs security acceleration access optimization	The manual access of Mini Programs Security Acceleration supported hybrid access for both native mini programs and embedded H5 development, enabling protection for hybrid-developed mini programs. Mobile Mini Programs Security access supported one-click automatic access and publishing, as well as one-click unpublishing, improving access efficiency and user experience.	2023-12-25	-

November 2023

Update	Description	Release Date	Documentation
Enhanced BOT protection scenes	Spam SMS and Email bombing scene: This scene defended against large-scale spam SMS and email bombing. When a business account was targeted by such attacks, it was recommended to select this scene and customize the protection scope to include the relevant URLs being bombarded. Social media flooding scene: This scene defended against automated actions such as registration, comments, and likes. When your social media ecosystem was disrupted by these automated behaviors of your businesses, it was recommended to select this scene and customize the protection scope to include the relevant URLs.	2023-11-20	-

	Automated download scene: This scene defended against automated software/app downloads and attacks on download sites. When your business experienced a high volume of automated downloads or attacks on download sites, it was recommended to select the Automated Download Scene and customize the protection scope to include download-related URLs. Custom scene: This scene allowed you to customize protection policies based on the specific characteristics of your business. When you needed policies that suited your unique business needs, it was recommended to select the Custom Scene. If you had any questions during the configuration process, see the Practical Tutorial Documentation.		
Security overview report optimization	A new domain name QPS peak Top 5 analysis chart had been added, enabling quick identification of abnormal domain names and URLs during sudden business traffic surges.	2023-11-20	Security Overview
Basic security rule configuration optimization	Access control and precise allowlist rule copy optimization: When rules were copied to other domain names, a new copy only new rules feature had been added, supporting incremental copying needs and reducing the risk of accidental operations. Access control rule configuration optimization: The batch protection module supported access control configuration, allowing rapid deployment of ACL rules to multiple domain names.	2023-11-20	Basic Security
API security support for custom API asset aggregation policies	For specific API paths, matching was performed based on the entered regular expressions: No configuration was required by default; if not customized, API aggregation would follow the system's built-in model. Since API aggregation was closely related to the user's actual business design, it was difficult to avoid a few cases where API asset aggregation may not meet user expectations. In such instances, custom aggregation rules could be used to adjust the aggregation results. Once a custom aggregation rule was matched, the next asset update would discard historical data and display results based on the latest aggregation.	2023-11-20	API Security
Mini programs security	The WeChat gateway access linkage had been established, providing native high-availability acceleration services. In weak network environments, transmission speed was	2023-11-15	-

acceleration feature release	improved by 300%, and network success rates were increased to over 99.9%. By combining WeChat security gateway with WAF security protection capabilities, native security protection was provided for mini programs against dozens of typical attacks, including DDoS protection, DNS hijacking prevention, anti-scraping, and anti-fraud measures. Ready to use, providing unified security management for both web and mini program platforms.		

September 2023

Update	Description	Release Date	Documentation
Support for hybrid cloud access and protection capabilities	By deploying containerized WAF protection nodes in various hybrid cloud web business scenes, such as other public clouds, on-premise IDCs, and server rooms, users could benefit from localized protection for multiple business operations. This setup offered security Ops capabilities consistent with Tencent Cloud WAF protection for web businesses. Additionally, it provided local protection and the same level of efficient, convenient, and secure protection and management capabilities as cloud WAF for web businesses that had not yet migrated to the cloud.	2023-09-27	-
Protection experience optimization	CC protection supported multiple SESSION configurations: You could configure multiple SESSION settings and customize which SESSION setting to apply when creating new rules, meeting the need to recognize various session IDs when multiple clients accessed the website. IP allowlist and blocklist supported one-click clearing of expired rules.	2023-09-27	Basic Security
Addition of easy mode support in BOT management	A built-in expert-managed BOT detection rule set with a false positive rate of less than 0.05% was available, enabling precise identification of suspicious BOT features and quick activation of the interception mode.	2023-09-27	-
BOT protection capability and	New BOT protection scenes for scanning and critical protection had been added, helping users defend against automated malicious scanning attacks and quickly strengthen protection during critical periods.	2023-09-27	BOT Management

experience upgrades	Optimization of BOT management experience: Custom rules supported the addition of an IP location field, allowing for more granular protection configurations. BOT traffic analysis report included abnormal request trend statistics, making abnormal traffic analysis more intuitive. BOT details could be exported, making statistical analysis more convenient. Attack log rule management supported BOT custom rule types. When a custom rule was triggered, you could quickly access rule details and make adjustments of the content directly within the interface.		
API security support for custom sensitive data detection rules	API security supported custom sensitive data detection rules, providing three matching methods: keyword matching, character matching, and regular expression matching. This enabled precise identification of sensitive APIs, facilitating their remediation.	2023-09-27	API Security
Overview and CLS experience optimization	The overview page displayed options for auto-renewal and upgrades for instances, as well as renewal and upgrade links for the Cloud Log Service, enhancing the user experience for upgrades and renewals. The overview page provided basic security analysis, including attack interception statistics related to web security protection, access control, and CC attack protection, along with week-over-week data analysis and corresponding interception trend analysis. Users could also click to view detailed attack logs, enhancing the basic security report experience. Attack and access log fields had been optimized to support TOP 50 results statistics in both ascending and descending order, assisting ops analysis.	2023-09-27	Security Overview

August 2023

Update	Description	Release Date	Documentation
Access capability upgrade	Grayscale support for cloud-native API Gateway traffic access: Users could configure traffic from cloud-native API gateways for protection through load-balancing WAF, as well as migrate CLB instance traffic for access.	2023-08-25	Domain Name Management

	Grayscale support for object access had been introduced for private network CLB instance access protection and private network CLB domain name access protection in regions outside the Chinese mainland. Custom resettings of XFF capability supported for users: If it was confirmed that there were no proxy service before WAF, users could clear the XFF field to prevent access from maliciously spoofed traffic, further enhancing business security. For domain name access, the round-robin scheduling policy supported setting the weight to 0, enabling smooth origin-pull switching to different nodes in multi-site active-active scenes.		
Protection capability upgrade	Grayscale support for regular expression rule configuration: Certain fields in basic security custom rules and BOT custom rules supported regular expression configuration. (This feature was available for Enterprise Edition and later editions of WAF instances upon requests for grayscale rollout.) The execution methods for precise allowlists and IP allowlists had been optimized. Regional blocking supported batch protection settings: You could apply the same region blocking policy to multiple domain names simultaneously. Supported BOT protection information transmission: After BOT traffic management was enabled in SaaS-based WAF, the BOT protection information transmission feature could be flexibly activated. This allowed BOT scores and client unique IDs to be inserted into HTTP headers and returned to the origin server. The origin server could then use this information to customize secondary handling policies, supporting business protection needs. Addition of UA policy module in BOT Traffic Management - Intelligent Analysis: This feature allowed users to customize which UA types to enable or disable for analysis, facilitating more refined management of UA policies. Optimized BOT Traffic Management - Custom Rule Configuration Experience: A new Header parameter value field had been added, allowing actions to be configured based on specific request content. Additionally, string-type matching fields supported multiple matching content entries separated by carriage returns.	2023-08-25	-
User experience optimization	Domain name list experience optimization: Supported batch enabling and disabling of access logs and API security switches.	2023-08-25	Domain Name Management

	Supported fuzzy retrieval of origin server domain names to retrieve accessed domain name information, enhancing the retrieval experience. Supported exporting configuration information corresponding to domain names, improving the analysis experience when you checked configurations across multiple domain names in large-scale access scenes. The API security user experience had been optimized to support quick analysis of API assets across all domain names and to analyze recent access trends for these assets. API Traffic Analysis, API Asset Management, and API Event Management supported viewing from an **All Domains** perspective. The API asset list supported viewing and downloading the call volume for the past 30 days. Click **View API Asset Details** to view the QPS peak for the previous day. Log shipping supported selecting CKafka as a target environment with SASL PLAINTEXT for encrypted authentication before shipping.		
Result visualization optimization	The security overview page allowed report filtering and viewing with minute-level granularity. When the selected time period was less than 6 hours, the business analysis curve chart was refined to a 30-second time granularity. Attack log field optimization: Two new fields, Scene ID and Scene Module, had been added. These allowed users to quickly locate the specific rule triggered by an attack using the Scene ID, Scene Module, and Rule ID fields. The status field had been modified to support filtering by action types, including Intercept, Monitor, CAPTCHA, and Redirect. A new sec_chain field had been added, allowing users to view the modules a request passed through and the actions executed by each module. A new prote_domain field had been added to display the accessed domain name or CLB object. This allowed for the addition of corresponding false positive correction allowlists or source IP blocklists, supporting quick handling of traffic for wildcard domain names, object access, and default domain name scenes. The BOT Traffic Analysis Report experience had been optimized to allow for clearer filtering and more detailed BOT statistics. HTTP response code filtering had been added.	2023-08-25	Attack Logs

	Customization of BOT detail list fields was supported. The View BOT Details - Request Feature Information module included the scoring information for each BOT module.		
Elastic postpaid billing support for BOT management	Elastic QPS billing supported extended BOT protection: After the elastic billing and BOT protection were enabled, any business request peaks that exceeded the total QPS quota purchased for the instance would incur an additional charge of USD 0.02 per QPS per day.	2023-08-25	Billing Overview

May 2023

Update	Description	Release Date	Documentation
Access capability upgrade	Object access capabilities had been upgraded to support all IPv6 CLB instances, and WAF instances outside the Chinese mainland could enable object access.	2023-05-31	-
Protection capability upgrade	CLB-WAF instances supported customizing response status code configurations.	2023-05-31	-
Comprehensive user experience upgrade	Multi-instance domain name access optimization: The domain name access quantity reminders and instance purchase notifications had been optimized, enhancing the overall service experience. Domain name access was case-insensitive, preventing missed interceptions due to case differences and enhancing protection effectiveness. The Rule ID field in attack logs supported viewing and editing related custom rules, enhancing the user experience.	2023-05-31	Attack Logs

April 2023

Update	Description	Release Date	Documentation
Access capability	CLB-WAF supported the protection of private network-based CLB web business.	2023-04-27	-

upgrade			
Comprehensive user experience upgrade	The management of instance overage and renewal consistency reminders had been upgraded and improved, ensuring greater service stability. API performance and OpenAPI documentation had been upgraded and improved, ensuring stability and ease of use for third-party calls. Emergency CC protection capabilities had been optimized and upgraded, improving both protection effectiveness and user experience. CLB-WAF supported automated emergency CC protection, effectively ensuring business availability. Monitoring capabilities had been upgraded to support the monitoring and alarming of various metrics at the WAF instance level.	2023-04-27	-
Major release of API Security 2.0	After API security was enabled, you could activate API security analysis for accessed domain names with a single click. This helped businesses identify API risks and sensitive data, effectively reducing API exposure and building an intelligent and precise API security defense system.	2023-04-24	-

June 2022

Update	Description	Release Date	Documentation
Launch of SaaS-based WAF in a new region	SaaS-WAF supported 9 new nodes in Singapore, Bangkok, Jakarta, Seoul, Tokyo, Silicon Valley, Frankfurt, Virginia, and São Paulo.	2022-06-03	-
Launch of CLB-based WAF in a new region	CLB-based WAF supported multiple new nodes.	2022-06-03	-
Cross-regional simultaneous upgrade support	Web Application Firewall supported simultaneous upgrades across regions, including both Chinese mainland and non-mainland regions, enhancing user experience and optimizing product capabilities.	2022-06-03	-

Experience upgrade	The data storage for Web Application Firewall instances outside the Chinese mainland had been optimized to support isolated viewing of resource data by region, enhancing the user operation and management experience.	2022-06-03	-
Access experience optimization	Access capabilities had been optimized, enhancing user access stability and experience.	2022-06-03	-

April 2022

Update	Description	Release Date	Documentation
Operation logs	The console supported viewing Web Application Firewall operation audit logs, as well as user operation queries and traceability.	2022-04-29	-
Instance list	Users could purchase multiple editions or upgrade across different editions of Web Application Firewall instances, allowing them to select the appropriate edition based on their specific business protection needs.	2022-04-29	Upgrade Method
Access mode	In the origin-pull mode, users could customize the configuration of multiple IP weighted round-robin scheduling settings, meeting the load balancing needs for complex SaaS-based accesses.	2022-04-29	Domain Name Addition
Precise allowlist rule optimization	Precise allowlist rules supported allowlisting custom rules (access control), enhancing granular traffic management capabilities.	2022-04-29	Precise Allowlist
Protection capability optimization	Enhanced protection capabilities for ultra-long messages had been added, improving protection, reducing missed interceptions, and optimizing the protection experience. The protection capabilities for attack patterns in the header Connection had been enhanced, reducing missed interceptions and improving overall protection.	2022-04-29	-
Log shipping service	The log shipping feature allowed log data to be shipped to CLS or TDMQ for CKafka, helping to uncover the value of log data and assisting users in addressing log Ops needs.	2022-04-10	Log Shipping
New BOT	A new BOT session management feature had been added,	2022-04-	-

session management	which optimized BOT protection capabilities by parsing session traffic types.	01	
BOT traffic analysis optimization	BOT traffic analysis had been enhanced by collecting data from BOT behavior management. This allowed for a quick understanding of the impact of BOTs on selected and enabled domain names. Users could rapidly access information on the current BOT classification trends, handling trends, BOT score distribution, top request volume statistics, and a list of vulnerable asset URLs.	2022-04-01	BOT Traffic Analysis
BOT traffic details optimization	BOT traffic analysis collected data from BOT behavior management, allowing for a quick understanding of the impact of BOTs on selected and enabled domain names. Users could click to view details, see BOT information related to specific access sources, identify access patterns, and detect any exceptions associated with BOT from those sources.	2022-04-01	BOT Traffic Details

March 2022

Update	Description	Release Date	Documentation
Enhanced IP blocking capability	IP blocking supported domain name-level differentiated blocking, allowing different detection duration and separately calculated blocking time for each domain name.	2022-03-02	IP Blocking Penalties

January 2022

Update	Description	Release Date	Documentation
BOT and business security	A new custom BOT session policy had been introduced.	2022-01-02	-
BOT and business security	BOT protection supported integration with App CAPTCHA.	2022-01-02	Accessing WAF CAPTCHA at Frontend-Backend

			Separated Sites

Product Announcement
Adjusting Billing of WAF BOT Traffic Management

Last updated：2023-09-08 18:22:07

WAF plans to adjust the billing of BOT traffic management fees starting from October 11, 2023.
Updates are as follows:
Before adjustment: The BOT traffic management fee is billed independently from the WAF instance, with a quota of 2500 QPS per month. For out-of-plan QPS, you can purchase extra packages (750 USD/1000 QPS/month).
After adjustment: The BOT traffic management fee is billed together with the WAF instance. It shares the QPS quota of the WAF instance. The QPS quota varies by the instance edition. The selling of extra packages for BOT traffic management stops. For out-of-plan QPS, you can purchase extra capacity packages at a price of 275 USD/1000 QPS/month (for Chinese mainland regions) or 300 USD/1000 QPS/month (for regions outside the Chinese mainland).
The above policy starts canary release gradually from September 2023, and will be officially launched from October 11, 2023. Thanks for your support. If you have any questions, please contact us.

Announcements

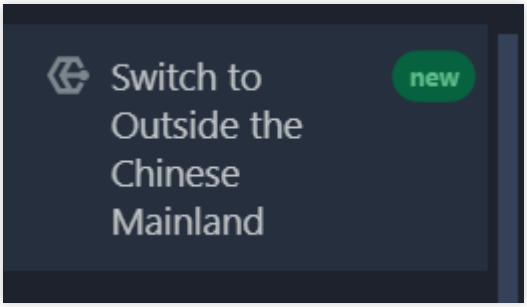
Last updated：2022-09-19 10:36:43

Release Notes at Tencent Cloud International

To improve the business connection and protection configuration experience outside the Chinese mainland, WAF was upgraded on June 2, 2022, with the web console 2.0 released. After the upgrade, connection is more stable, protection is more powerful, and traffic management is more refined, with value-added capabilities of bot traffic management and log service supported. In addition, the console allows you to switch between regions in and outside the Chinese mainland to better manage instance resources by region.
Different types of WAF instances are impacted as follows:
SaaS WAF: The region attributes of WAF instances remain unchanged, the system automatically adds region fields according to the attributes, and the console supports management by region.
CLB WAF: WAF instances in the Chinese mainland support connecting and protecting web businesses for CLB instances in the Chinese mainland, and those outside the Chinese mainland support those of CLB instances outside the Chinese mainland.
After **this** upgrade to web console 2.0, you can enjoy the following product capabilities and configurations:

Cross-region resource data isolation

The console allows you to switch between regions in and outside the Chinese mainland as shown below:



More convenient domain name connection

Upgraded domain name connection and management

You can manage multiple instances in a unified manner to improve the routine security Ops efficiency. SaaS WAF instances support custom weight-based IP forwarding as well as multi-domain name forwarding to enable complex business connections.

Domain name connection guide

A domain name connection guide is added, providing more detailed directions after a domain name is added and facilitating business connection.

Custom traffic tagging

SaaS WAF instances support custom traffic tagging to meet the requirements of more complex business analysis and linked protection.

Client information logging

SaaS WAF instances allow you to enable the transfer of business client source IP address and port information. This complements XFF records to ensure business compliance in finance and ecommerce industries.

Protection capability upgrade

Quick protection switch

You can quickly enable or disable all protection modules and certain features of certain protection modules. This facilitates routine Ops troubleshooting, accelerates problem locating, and ensures business continuity.

Refined traffic management

IP blocklist/allowlist is upgraded to blocklist/allowlist management. Custom policy rules that were previously set to "allow" are upgraded to precise allowlist rules, and other custom policy rules are upgraded to access control rules. Rule configuration and execution are not affected by the upgrade.

The precise allowlist feature implements refined traffic management during routine security Ops, improving the traffic control efficiency and effect while ensuring business security.

Value-added capability upgrade - commercial release of bot traffic management

The newly upgraded bot protection system integrates the browser bot defense module, threat intelligence module, as well as big data and AI algorithm model and analysis engine. It provides visualized traffic analysis by risk level and more intuitive threat handling policies.

Security Advisory
Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44832)

Last updated：2022-06-23 11:14:26

On December 29, 2021, Tencent Cloud Security Operations Center noticed that **Apache Log4j 2 announced that there was a remote code execution vulnerability (CVE-2021-44832) in some special scenarios. The vulnerability is hard to exploit, as attackers can remotely execute arbitrary code only if they have permissions to modify the configuration file.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is an open-source Java-based logging framework. As an upgraded version of Log4j 1.x, it rewrites the Log4j framework and introduces various new features, making it widely suitable for logging in the development of many business systems.

As described by Apache, attackers with permissions to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code

As this vulnerability requires that attackers have the permission to modify configuration files (which usually can be implemented only through other vulnerabilities) and doesn't exist in the default configuration, it is hard to exploit.

Risk Level

Medium.

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

2.0-beta7 ≤ Apache Log4j 2.x < 2.17.0 (excluding 2.3.2 and 2.12.4)

Safe Versions

- Apache Log4j 2.x ≥ 2.3.2 (Java 6)
- Apache Log4j 2.x ≥ 2.12.4 (Java 7)
- Apache Log4j 2.x ≥ 2.17.1 (Java 8 or later)

Suggestions for Fix

Currently, an official safe version of Apache Log4j 2 has been released. You can update to it as instructed in Download Apache Log4j 2.

> Note：
> Back up your data before upgrading to avoid accidental losses.

Tencent Security Solution

Tencent Cloud NTA rule libraries released after December 29, 2021 support detecting the Log4j 2 RCE vulnerability CVE-2021-44832.

References

For more information, see Apache Log4j Security Vulnerabilities.

Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-45046)

Last updated：2022-06-23 11:14:26

On December 17, 2021, Tencent Cloud Security Operations Center noticed that **Apache Log4j's fix for CVE-2021-44228 was incomplete in non-default configurations, so the vulnerability could be exploited by attackers to launch remote code execution attacks in some special configuration scenarios.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is an open-source logging component as the upgrade of Apache Log4j. It controls the output format of each log and allows you to define the level of each log to control the log generation process in a more refined manner.

After disclosing the severe RCE vulnerability CVE-2021-44228 on December 9, 2021, **Apache Log4j recently disclosed another RCE vulnerability CVE-2021-45046, whose severity increased from CVSS 3.7 to CVSS 9.0. This vulnerability is caused by the incomplete fix for CVE-2021-44228 in non-default configurations. In certain scenarios such as thread context search mode, attackers can construct specific requests to execute code remotely.**

This vulnerability also affects a high number of universal applications and components around the globe, such as:
Apache Struts 2
Apache Solr
Apache Druid
Apache Flink
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
Elasticsearch
Logstash
...
We recommend you check and upgrade all systems or applications that use the Log4j component in time.

Risk Level

High (CVSS score: 9.0)

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

2.0-beta9 ≤ Apache Log4j 2.x < 2.16.0 (excluding 2.12.2)

Safe Versions

- Apache Log4j 2.16.0 (Java 8)
- Apache Log4j 2.12.2 (Java 7)

Suggestions for Fix

We recommend you conduct internal inspections to check whether your business applications use the Apache `log4j-core` JAR package. If the dependency is introduced and the Log4j version is among the affected versions, the vulnerability may affect your business, and you can take the following measures:

> Note：
> Back up your data before upgrading to avoid accidental losses.

Upgrading to latest official version (recommended)

Currently, officially fixed versions have been released. You can upgrade the component or update the code to this version.

- If you use Java 8, upgrade to Apache Log4j 2.16.0.
- If you use Java 7, upgrade to Apache Log4j 2.12.2.

Using other protection solutions

1. If you cannot upgrade the version currently, we recommend you run the following command to remove the `JndiLookup` class file from the `log4j-core` package and restart the service:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

2. Use a security group or firewall to restrict the affected applications from accessing the internet.

References

For more information, see Apache Log4j Security Vulnerabilities.

Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44228)

Last updated：2022-06-23 11:14:26

On December 9, 2021, Tencent Cloud Security Operations Center noticed that **a severe code execution vulnerability (CVE-2021-44228) in Apache Log4j 2 was disclosed. Currently, Log4j 2 has released an official security announcement and safe version. Once the vulnerability is exploited, problems such as server intrusion can occur.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is a widely used open-source logging component. It substitutes for print statements such as `System.out` in projects and is the most popular logging tool in Java.

If Log4j 2 is used to process malicious data in certain scenarios, malicious code may be injected and executed.

Log4j 2 is used by many Java frameworks and applications as a third-party basic logging library. Your business may be attacked through this vulnerability if it uses Log4j 2 to output logs and the log content can be partially controlled by attackers. Therefore, this vulnerability also affects a high number of universal applications and components around the globe, such as:
Apache Struts 2
Apache Solr
Apache Druid
Apache Flink
Apache Flume
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
Elasticsearch
Logstash
...
We recommend you check and upgrade all systems or applications that use the Log4j component in time.

Risk Level

High Risk

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

Apache Log4j 2.0–2.14.1

Safe Versions

Apache Log4j 2.16.0

Suggestions for Fix

Upgrading to latest official version (recommended)

The current latest official version is log4j-core-2.16.0. You can upgrade the component or update the code to this version.

Disabling lookup feature in Log4j

Disabling in configuration file (recommended)

Add the following content to the `log4j2.component.properties` configuration file (if it doesn't exist, manually create one) in `classpath` of Log4j 2.9.1 or later:

```
log4j2.formatMsgNoLookups=True
log4j.formatMsgNoLookups=True
```

Disabling through JVM parameter configuration (not recommended as the configuration can be easily lost)

Add `-Dlog4j2.formatMsgNoLookups=true` and `-Dlog4j.formatMsgNoLookups=true` to the JVM startup parameters.

Note：
For versions 2.0–2.10, you should upgrade them to 2.10 or later first and then add JVM parameters.

Upgrading JDK to later versions (recommended)

As JDK on a later version has some security limits, we recommend you upgrade JDK to 6u211, 7u201, 8u191, or 11.0.1 or later. This can block vulnerability exploit methods such as JNDI to a certain extent.

Other temporary mitigation measures

You can use a firewall or security group to prohibit relevant applications and businesses from actively connecting to the public network.

Tencent Security Solution

Tencent Cloud WAF can detect and block attacks exploiting the Log4j 2 RCE vulnerability.

References

For more information, see Apache Log4j Security Vulnerabilities.

Notice for WebLogic Console HTTP RCE Vulnerability

Last updated：2022-06-23 11:14:26

Vulnerability Details

On October 20, 2020, Tencent Security noticed that Oracle released a patch update advisory. It revealed WebLogic vulnerabilities, among which CVE-2020-14882 and CVE-2020-14883 existed in the WebLogic console, a default component on all WebLogic versions. Attackers can exploit CVE-2020-14882 and CVE-2020-14883 to execute arbitrary code on the server, obtain system permissions, and control the server without authorization, compromising data confidentiality, integrity, and availability.
All Tencent Security services have upgraded rules and vulnerability libraries accordingly to prevent attacks.
To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Risk Level

High Risk

Vulnerability Risk

Attackers can exploit the vulnerabilities to control Oracle WebLogic Server, compromising data confidentiality, integrity, and availability.

Affected Versions

Oracle WebLogic Server 10.3.6.0.0
Oracle WebLogic Server 12.1.3.0.0
Oracle WebLogic Server 12.2.1.3.0
Oracle WebLogic Server 12.2.1.4.0
Oracle WebLogic Server 14.1.1.0.0

Suggestions for Fix

A new version has been officially released to fix the vulnerabilities. Tencent Security recommends you:

Recommendation solution: Install the patch in time.

Use WAF to block similar WebLogic vulnerability attacks.

References

For more information, see Oracle Critical Patch Update Advisory - October 2020.

Notice for Exchange Server Command Execution Vulnerability

Last updated：2022-06-23 11:14:26

On September 17, 2020, Tencent Security noticed that Microsoft issued a security advisory for a command execution vulnerability in Exchange Server (CVE-2020-16875).

Note:

Microsoft Exchange Server is an email service program offered by Microsoft Corporation, which provides various features such as mail access, storage, forwarding, voice mail, and mail filtering.

The POC of the vulnerability is being circulated on the internet. Tencent Security recommends you upgrade Exchange to the latest version in time and implement asset inspection and protection to avoid attacks by hackers. Tencent Cloud WAF currently supports defense against them.

Vulnerability Details

A remote code execution vulnerability exists in Microsoft Exchange Server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires successful authentication by Exchange. As the Exchange service ran with SYSTEM privileges, an attacker could get the highest privileges of the system by exploiting this vulnerability.

Affected Versions

Microsoft Exchange Server 2016 Cumulative Update 16
Microsoft Exchange Server 2016 Cumulative Update 17
Microsoft Exchange Server 2019 Cumulative Update 5
Microsoft Exchange Server 2019 Cumulative Update 6

Suggestions for Fix

According to the vulnerability advisory, Tencent Security recommends you:
Update to the latest version for fix in time.
Use WAF to detect and block attacks.

References

CVE-2020-16875

Notice for Yonyou GRP-U8 SQL Injection Vulnerability

Last updated：2022-06-23 11:14:26

On September 11, 2020, Tencent Security noticed a SQL injection vulnerability in Yonyou GRP-U8 internal control and management software for government affairs. Attackers can use a carefully constructed payload to perform SQL injection attacks in order to get sensitive database information.
Exploitations in the wild (ITW) have been detected, and Tencent Cloud WAF supports defense against them.

Vulnerability Details

Attackers can use a carefully constructed payload to perform SQL injection attacks in order to get sensitive database information, and Tencent Cloud WAF currently supports defense against them.

Affected Versions

Yonyou GRP-U8 internal control and management software for government affairs.

Suggestions for Fix

According to the vulnerability advisory, there is currently no official update. Tencent Security recommends you:
Restrain exposing the software to the public network due to its sensitivity or use an allowlist policy.
Use WAF to detect and block attacks.

References

CNVD-2020-49261
Yonyou Gov website

Notice for Apache Cocoon XXE Vulnerability (CVE-2020-11991)

Last updated：2022-06-23 11:14:26

On September 11, 2020, the Apache Software Foundation issued a security advisory to fix the XXE vulnerability in Apache Cocoon (CVE-2020-11991).

Vulnerability Details

Apache Cocoon is a Spring-based framework built around the concepts of separation. All processing jobs under it are linearly connected by predefined processing components, which can process the inputs and generated outputs in a pipeline sequence. Its users include Apache Lenya, Daisy CMS, Hippo CMS, Mindquarry, etc. It is usually used as a data ETL tool or relay for data transfer between systems.
CVE-2020-11991 is related to StreamGenerator. When using the StreamGenerator, Cocoon parses a user-provided XML. A specially crafted XML, including external system entities, could be used to access any file on the server system.

Risk Level

High Risk

Vulnerability Risk

A specially crafted XML, including external system entities, could be used to access any file on the server system.

Affected Versions

Apache Cocoon <= 2.1.12

Suggestions for Fix

The vulnerability has been officially fixed in the new version. Tencent Security recommends you:

Upgrade to the latest version (2.1.13) of Apache Cocoon.

Use Tencent Cloud WAF that supports detection of and defense against XXE vulnerabilities like CVE-2020-11991.

Note:

Back up your data before installing the patch to avoid accidental losses.

References

Official update notice:

Apache Cocoon

Apache Cocoon 2.2

CVE-2020-11991

Notice for WordPress File Manager Arbitrary Code Execution Vulnerability

Last updated：2022-06-23 11:14:27

On September 6, 2020, Tencent Security noticed an arbitrary code execution vulnerability in the File Manager plugin of WordPress. Attackers can exploit this vulnerability to upload trojans and run arbitrary commands and malicious scripts on WordPress websites that contain File Manager.
Tencent Security has captured exploitations in the wild (ITW), and Tencent Cloud WAF currently supports defense against them.

Vulnerability Details

Tencent Security noticed an arbitrary code execution vulnerability in the File Manager plugin of WordPress. Attackers can exploit this vulnerability to upload trojans and run arbitrary commands and malicious scripts on WordPress websites that contain File Manager. In the plugin library of wordpress.org, the version 6.8 provided by File Manager before September 1, 2020 is the affected version, which can be used by attackers to damage websites.
File lib/php/*.php can be by default opened directly, and this file loads lib/php/*.php which reads POST/GET variables, and then allows executing some internal features, like uploading files. PHP is allowed, thus this leads to unauthenticated arbitrary file upload and remote code execution.

Affected Versions

WordPress File Manager < 6.9

Suggestions for Fix

An upgraded plugin has been officially released to fix this vulnerability. Tencent Security recommends you:
Update WordPress File Manager to 6.9 or later.
Use WAF to detect and block attacks.

References

CVE 2020-25213

Jenkins Security Advisory for September

Last updated：2022-06-23 11:14:27

On September 3, 2020, Tencent Security noticed that Jenkins issued its security advisory for September, which contained 14 CVE vulnerabilities (CVE-2020-2238, CVE-2020-2239, CVE-2020-2240, CVE-2020-2241, CVE-2020-2242, CVE-2020-2243, CVE-2020-2244, CVE-2020-2245, CVE-2020-2246, CVE-2020-2247, CVE-2020-2248, CVE-2020-2249, CVE-2020-2250, and CVE-2020-2251) with 10 plugins affected, including:
Build Failure Analyzer Plugin
Cadence vManager Plugin
database Plugin
Git Parameter Plugin
JSGames Plugin
Klocwork Analysis Plugin
Parameterized Remote Trigger Plugin
SoapUI Pro Functional Testing Plugin
Team Foundation Server Plugin
Valgrind Plugin
The following vulnerabilities are defined as high for severity:
CVE-2020-2248 (XSS vulnerability in JSGames Plugin)
CVE-2020-2247 (XXE vulnerability in Klocwork Analysis Plugin)
CVE-2020-2246 (XSS vulnerability in Valgrind Plugin)
CVE-2020-2245 (XXE vulnerability in Valgrind Plugin)
CVE-2020-2244 (XSS vulnerability in Build Failure Analyzer Plugin)
CVE-2020-2243 (Stored XSS vulnerability in Cadence vManager Plugin)
CVE-2020-2240 (CSRF vulnerability in database Plugin)
CVE-2020-2238 (Stored XSS vulnerability in Git Parameter Plugin)
Jenkins is an open-source automated middleware project based on Java for continuous integration and delivery and is commonly used in the development process. To avoid impact on your business, Tencent Security recommends you conduct a security inspection in time. If your business is affected, update and fix the vulnerabilities promptly to prevent intrusions by attackers. As some vulnerabilities have no fixes yet, we recommend you use Tencent Cloud WAF for defense.

Vulnerability Details

Stored XSS vulnerability in Git Parameter Plugin (CVE-2020-2238)

Git Parameter Plugin 0.9.12 and earlier do not escape the repository field on the "Build with Parameters" page. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.
This vulnerability is fixed on Git Parameter Plugin 0.9.13.
Secret stored in plaintext by Parameterized Remote Trigger Plugin (CVE-2020-2239).
Parameterized Remote Trigger Plugin 3.1.3 and earlier store a secret in plaintext.

CSRF vulnerability in database Plugin (CVE-2020-2240)

database Plugin 1.6 and earlier do not require POST requests for the database console, resulting in a cross-site request forgery (CSRF) vulnerability. This vulnerability allows attackers to execute arbitrary SQL scripts.
CSRF vulnerability and missing permission checks in database Plugin (CVE-2020-2241 (CSRF), CVE-2020-2242 (permission check)).
database Plugin 1.6 and earlier do not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read access to Jenkins to connect to an attacker-specified database server using attacker-specified username and password. Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability.
database Plugin 1.7 requires POST requests and Overall/Read permission for the affected form validation method.

Stored XSS vulnerability in Cadence vManager Plugin (CVE-2020-2243)

Cadence vManager Plugin 3.0.4 and earlier do not escape build descriptions in tooltips. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission.
Cadence vManager Plugin 3.0.5 removes affected tooltips.

XSS vulnerability in Build Failure Analyzer Plugin (CVE-2020-2244)

Build Failure Analyzer Plugin 1.27.0 and earlier do not escape matching text in a form validation response. This results in a cross-site scripting (XSS) vulnerability exploitable by attackers able to provide console output for builds used to test build log indications.
Build Failure Analyzer Plugin 1.27.1 escapes matching text in the affected form validation response.

XXE vulnerability in Valgrind Plugin (CVE-2020-2245)

Valgrind Plugin 0.28 and earlier do not configure the XML parser to prevent XML external entity (XXE) attacks. This allows a user able to control the input files for the Valgrind Plugin parser to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.
As of publication of this advisory, there is no fix.

XSS vulnerability in Valgrind Plugin (CVE-2020-2246)

Valgrind Plugin 0.28 and earlier do not escape content in Valgrind XML reports. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control Valgrind XML report contents.
As of publication of this advisory, there is no fix.

XXE vulnerability in Klocwork Analysis Plugin (CVE-2020-2247)

Klocwork Analysis Plugin 2020.2.1 and earlier do not configure the XML parser to prevent XML external entity (XXE) attacks. This allows a user able to control the input files for the Klocwork plugin parser to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.
As of publication of this advisory, there is no fix.

Reflected XSS vulnerability in JSGames Plugin (CVE-2020-2248)

JSGames Plugin 0.2 and earlier evaluate part of a URL as code. This results in a reflected cross-site scripting (XSS) vulnerability.

As of publication of this advisory, there is no fix.

Credentials stored in plaintext by Team Foundation Server Plugin (CVE-2020-2249)

Team Foundation Server Plugin 5.157.1 and earlier store a webhook secret unencrypted in the global configuration file hudson.plugins.tfs.TeamPluginGlobalConfig.xml on the Jenkins controller as part of the configuration. This secret can be viewed by attackers with access to the Jenkins controller file system.

Passwords stored in plaintext by SoapUI Pro Functional Testing Plugin (CVE-2020-2250)

SoapUI Pro Functional Testing Plugin 1.3 and earlier store project passwords unencrypted in job config.xml files as part of the configuration. These project passwords can be viewed by attackers with Extended Read permission or access to the Jenkins controller file system. SoapUI Pro Functional Testing Plugin 1.4 stores project passwords encrypted once affected job configurations are saved again.

Passwords transmitted in plaintext by SoapUI Pro Functional Testing Plugin (CVE-2020-2251)

SoapUI Pro Functional Testing Plugin stores project passwords in job config.xml files on the Jenkins controller as part of the configuration.

While these passwords are stored encrypted on disk since SoapUI Pro Functional Testing Plugin 1.4, they are transmitted in plaintext as part of the global configuration form by SoapUI Pro Functional Testing Plugin 1.5 and earlier. These passwords can be viewed by attackers with Extended Read permission.

This only affects Jenkins earlier than 2.236, including 2.235.x LTS, as Jenkins 2.236 introduces a security hardening that transparently encrypts and decrypts data used for a Jenkins password form field.

As of publication of this advisory, there is no fix.

Risk Level

CVE-2020-2249: Low

CVE-2020-2239: Low

CVE-2020-2241: Medium

CVE-2020-2242: Medium

CVE-2020-2250: Medium

CVE-2020-2251: Medium

CVE-2020-2240: High

CVE-2020-2247: High

CVE-2020-2248: High

CVE-2020-2246: High

CVE-2020-2245: High

CVE-2020-2243: High

CVE-2020-2238: High
CVE-2020-2244: High

Affected Versions

Build Failure Analyzer Plugin <= 1.27.0
Cadence vManager Plugin <= 3.0.4
database Plugin <= 1.6
Git Parameter Plugin <= 0.9.12
JSGames Plugin <= 0.2
Klocwork Analysis Plugin <= 2020.2.1
Parameterized Remote Trigger Plugin <= 3.1.3
SoapUI Pro Functional Testing Plugin <= 1.3
SoapUI Pro Functional Testing Plugin <= 1.5
Team Foundation Server Plugin <= 5.157.1
Valgrind Plugin <= 0.28

Fixed Versions

Build Failure Analyzer Plugin should be updated to version 1.27.1
Cadence vManager Plugin should be updated to version 3.0.5
database Plugin should be updated to version 1.7
Git Parameter Plugin should be updated to version 0.9.13
Parameterized Remote Trigger Plugin should be updated to version 3.1.4
SoapUI Pro Functional Testing Plugin should be updated to version 1.4

Versions to Be Fixed

JSGames Plugin
Klocwork Analysis Plugin
SoapUI Pro Functional Testing Plugin
Team Foundation Server Plugin
Valgrind Plugin

Suggestions for Fix

Certain upgraded plugins have been officially released to fix these vulnerabilities; however, as some of them have no fix yet, Tencent Security recommends you:
Update the corresponding Jenkins plugins (as the plaintext storage vulnerability is a local vulnerability, you need to wait for the plugin update).
Restrain exposing Jenkins to the public network due to its sensitivity. If there is a need for public network access, you can configure an access policy such as IP allowlist in WAF.
Use WAF to detect and block network-based attacks through the vulnerabilities in the Jenkins Security Advisory for September.
WAF supports detection of and defense against all the vulnerabilities contained in the Jenkins Security Advisory for September.

References

The official advisories are as follows:
Jenkins Security Advisory 2020-09-01
CVE-2020-2238
CVE-2020-2239
CVE-2020-2240
CVE-2020-2241
CVE-2020-2242
CVE-2020-2243
CVE-2020-2244
CVE-2020-2245
CVE-2020-2246
CVE-2020-2247
CVE-2020-2248
CVE-2020-2249
CVE-2020-2250
CVE-2020-2251
XSS vulnerability in CloudBees Jenkins (CVE-2020-2246)
XSS vulnerability in CloudBees Jenkins (CVE-2020-2243)
XXE vulnerability in CloudBees Jenkins

Notice for Apache Struts 2 RCE Vulnerabilities (CVE-2019-0230 and CVE-2019-0233)

Last updated：2022-06-23 11:14:27

On August 13, 2020, Tencent Security noticed that Apache Struts issued a security advisory for the S2-059 Struts remote code execution vulnerability and S2-060 Struts denial of service vulnerability.

Vulnerability Details

Apache Struts 2 is a web framework for developing Java EE network applications.
S2-059 Struts remote code execution vulnerability (CVE-2019-0230): In cases such as improper use of certain tags, OGNL expression injection may exist, thereby causing a remote code execution vulnerability.
S2-060 Struts denial of service vulnerability (CVE-2019-0233): It may cause denial of service attacks when files are uploaded and manipulated.

Affected Versions

Apache Struts 2.0.0–2.5.20

Safe Versions

Apache Struts >= 2.5.22

Suggestions for Fix

Based on the vulnerability information, Tencent Security recommends you:
Upgrade the Apache Struts framework to the latest version.
Use Tencent Cloud WAF, an AI-based one-stop web security solution. The most typical characteristic of the S2-059 vulnerability is that it uses the OGNL language. The Tencent Security technical team conducted a targeted study on OGNL expressions, blocked attacks against such expressions, and integrated the defense capability into WAF. Therefore, as long as the vulnerability is attacked based on OGNL expressions, WAF can directly block them.
In addition, the intelligent engine of WAF also provides intelligent defense against SQL, XSS, and command execution

attacks. Backed by AI technologies, it can reasonably and effectively block unknown security vulnerabilities for improved business continuity.

References

Official advisory:

CVE-2019-0230

CVE-2019-0233

Notice for Apache SkyWalking SQL Injection Vulnerability (CVE-2020-13921)

Last updated：2022-06-23 11:14:27

On August 5, 2020, Tencent Force (force.tencent.com) researched and noticed that Apache SkyWalking had a SQL injection vulnerability (CVE-2020-13921). A new version has been officially released to fix this vulnerability.
To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers. For more information, see Affected Versions.

Vulnerability Details

Apache SkyWalking is an application performance monitor (APM) tool that provides automated and high-performance monitoring solutions for microservices, cloud native, and container-based applications. Its official website shows that it is being used by a large number of Chinese companies in the internet, banking, and civil aviation sectors.
In multiple versions of SkyWalking, unauthorized GraphQL APIs are opened by default, through which attackers can construct malicious request packets for SQL injection, resulting in the leakage of sensitive information in the user database. In view of the greater impact of this vulnerability, we recommend you fix it as soon as possible.

Risk Level

High Risk

Vulnerability Risk

Through SQL injection, attackers can steal sensitive information on servers.

Affected Versions

Apache SkyWalking 6.0.0–6.6.0
Apache SkyWalking 7.0.0
Apache SkyWalking 8.0.0–8.0.1

Fix

Apache SkyWalking 8.1.0

Suggestions for Fix

A new version has been officially released to fix this vulnerability. Tencent Security recommends you:
Recommended solution: Upgrade to Apache SkyWalking 8.1.0 or later.
Temporary mitigation: If the upgrade is temporarily impossible, as a mitigation measure, we recommend you restrain exposing the GraphQL APIs of Apache SkyWalking to the public network or add a layer of authentication on top of such APIs.
-**Recommendation for organizational users**: Use Tencent Security services to detect and block attacks through this Apache SkyWalking SQL injection vulnerability.
Tencent Cloud WAF supports detection of and defense against attacks through this SkyWalking SQL injection vulnerability.

References

If needed, you can find more information of the vulnerability here.