

WebApp Secure 5.5 Release Notes

Release Notes

Release 5.5
June 2014
Revision 2

These release notes accompany Release 5.5 of WebApp Secure. WebApp Secure protects websites from would-be attackers, fraud, and theft. Its Web intrusion prevention system uses deception to detect, track, profile, and block attackers in real time by inserting detection points into your webserver's output to identify attackers before they do damage. WebApp Secure then tracks detected attackers, profiling their behavior and deploying countermeasures.

For the latest, most complete information about outstanding and resolved issues with the WebAppSecure software, see the Juniper Networks online software defect search application at <http://www.juniper.net/prsearch>.

Contents

WebApp Secure 5.5 Release Overview	2
New and Changed Features	2
Installation Instructions	4
Downloading Updates	5
Downloading Documentation	5
Resolved Issues	5
Known Issues	6
Requesting Technical Support	7
WebApp Secure Documentation and Release Notes	8

WebApp Secure 5.5 Release Overview

The 5.5 release is a major release focusing on supportability and ease of administration, as well as improvements to the security feature set of the product. This release also has a number of enhancements and bug fixes aimed at improving:

- Performance
- Update processes
- Management interface usability
- Ease of configuration

New and Changed Features

Security

- Spotlight Connector—Feeds WebApp Secure fingerprint data to the SRX Series Services Gateway, making it possible for the SRX series to filter web traffic based on intelligence from WebApp Secure.
- Client Classification Processor—This processor, which identifies legitimate search engines and bots in order to white list their traffic patterns, has been enhanced so as to perform additional verification steps, mitigating potential side channel attacks on DNS.
- URL and Hostname Fuzzing—WebApp Secure now triggers security incidents on requests that contain invalid URI or hostname components as defined in RFC 3986. These requests are indicative of a user running an automated tool designed to find and exploit certain kinds of vulnerabilities.
- File Processor—There is a change to the default configuration to reduce the chance of false positives, based on real-world customer feedback and engineering team research.
- Error Processor—Rearchitecture of processor logic and change to the default configuration to reduce the chance of false positives and provide more security and less system resource consumption.
- Header Processor—Rearchitecture of processor logic and change to the default configuration to reduce the chance of false positives in AJAX-based web applications and provide more security.

Web UI

- Context Sensitive Help—Pages with corresponding help sections available in the administrator guide now have a link to these sections available on the page itself.
- Test Connection Settings—In the configuration sections of the Web UI where connections to external services are configured, there is now a button that enables administrators to test the connection from WebApp Secure to the external service without the need to save configuration. These buttons are available for backups push

to FTP, backups push to SSH, external counter response (SRX), SMTP, SNMP, Spotlight Secure, Spotlight Connector, and NTP.

- Configuration expert mode—Now allows searching by any word in the description of parameters.

Management and Supportability

- WebApp Secure now performs monitoring of key metrics related to services, attacker data, and system resources, and can be configured to send alerts via email or SNMP, as well as display this information in the Web UI.
- On hardware deployments, the RAID status may now be viewed in the Web UI.
- The “Services Status” pane of the “System Status” page of the Web UI now displays all services across the cluster, rather than just the local node that the Web UI is running on.
- The CLI now includes system settings, and this functionality has been reorganized.
- The ability to define a dedicated management interface is now provided.
- LDAP support has been changed to support both synchronous and asynchronous binding (formerly supported synchronous binding only), as well as LDAPS.
- SMTP support is enhanced to support STARTTLS as well as SMTPS (previously supported SMTPS only).
- If WebApp Secure requires a forward proxy to access the Internet or network resources, all parts of the system now allow proxy authentication.
- Any white list parameters (such as those used to configure a load balancer) will now accept CIDR notation instead of a non-standard “partial IP” format. Please see “Installation and Deployment Notes” before upgrading to 5.5.
- The mykonos-shell CLI is now accessible through the “cli” command.
- High Availability—Systems configured to use HA will now automatically failover when interfaces fail, and logic to prevent a serious “split brain” situation was added.
- Administrators may now define custom routing rules and routes from within the CLI.

Performance

- Restructured logic behind how HTML injections are performed, increasing throughput and decreasing system resource consumption.
- Database system will now be automatically vacuumed/cleaned under certain situations that might have previously caused speed issues and increased database size.

Installation Instructions

- The installation procedure for WebApp Secure remains the same. As soon as the update is available, it will be downloaded by the system automatically if the system is connected to the WebApp Secure Support System. If upgrading from version 5.1.0-x or lower, WebApp Secure system requires a reboot due to a change in the Linux Kernel. If upgrading from a version of 5.1.3, this reboot is not required.
- Due to a prior issue in the upgrade process, upgrading to WebApp Secure 5.5 requires that you first upgrade to version 5.1.3-32 or higher. If using the “online updates” method, this intermediary version will show up as an available update, and you will need to upgrade to it before the 5.5 release becomes available. If using the “offline updates” method, you will need to download and install the intermediary version manually.
- WebApp Secure 5.5 introduces the ability to have a dedicated management interface and multiple traffic Virtual IPs (VIPs) for High Availability pairs. With this change, the original VIP in versions prior to 5.5 is now considered the Management VIP, and is not considered valid for traffic purposes. If you were previously routing traffic to the VIP and using it as a listening IP for a defined application, you will need to modify your WebApp Secure configuration before performing the upgrade to version 5.5 or later. To determine if you need to make the changes or not, run the following command:
grep listen.ip_address /etc/mykonos/config.xml|grep -o \$(sudo mykonos-config -s ha -o vip) If there is no output from the command, no changes are needed and you are safe to continue with the upgrade. If you receive any output from the command (would be an IP address), then you will need to perform the following steps to upgrade WebApp Secure. Prior to performing these changes it is recommend you take WebApp Secure out-of-line.
 1. Change the listening ip addresses on any defined applications so that the virtual IP address is not included in the list. Because this is a temporary change, you can use other IPs you have associated with WebApp Secure.

If you are updating WebApp Secure live, you will need to update your upstream device(s) to route the traffic to the new addresses instead of the VIP to ensure zero downtime.
 2. Perform the upgrade to WebApp secure 5.5 as normal.
 3. If you would like to use the VIP you had originally defined as a Traffic VIP, you will need to add a new Management VIP first, using the following command from the shell:
cli system set management-vip <new mngt ip address>/<cidr netmask>

This will add a new Management VIP to the High Availability pair. Note: Ensure that the new Management IPs have been added to the WebApp Secure devices to properly set up the VIPs.
 4. You will need to add a new Traffic VIP using the following command from the shell:
cli system set traffic-vip traffic <ip address>/<cidr netmask>

5. Change the listening ip addresses for your application(s) to point to the new Traffic VIP.
 6. Update upstream device(s) to route traffic to the new Traffic VIP.
- Passwords for external services, such as SMTP servers and backup FTP or SSH servers, were previously stored in plain text. These values have been encrypted. Users who had these values set must re-set them after upgrading to 5.5.
 - If a customer has previously configured any of the “whitelist” parameters accessible through the Web UI’s **Configuration > Security Engine > Whitelists** section with a partial IP address, such as “192.168.” These must be unset manually prior to updating to 5.5, and then manually re-set using the new CIDR notation mentioned under the “Management and Supportability” heading. Failure to do this will result in the configuration updates present in this version to not be applied.
 - After an update to 5.5 is performed, the user must restart the “nginx” and “nginx_management” services. This may be performed on the command line with the commands **sudo /etc/init.d/nginx restart** and **sudo /etc/init.d/nginx_management restart**. This is necessary because this update of WebApp Secure contains performance and security updates to nginx that require the configuration files to be re-parsed. This must be performed on each node in a cluster or high availability deployment, in addition to on standalone systems.

Downloading Updates

- WebApp Secure systems not connected to WebApp Secure Support System: Visit <http://www.juniper.net/support/downloads/?p=jwas#sw> for obtaining the latest release tar file for update and follow offline update process
- WebApp Secure installations using AMI (Amazon Machine Image): Contact your sales engineering representative to gain access to the private AMI image

Downloading Documentation

The installed software update contains the new documentation. Documentation is also available at <http://www.juniper.net/support/downloads/?p=jwas#docs>

Resolved Issues

The following problems have been addressed for the current release of WebApp Secure.

- ETag Beacon Processor was found to cause multiple users of the same forward proxy server to be incorrectly associated and consolidated as one user, under certain proxy configurations.
- When multiple backend servers were configured, and one or more was configured as a “backup”, these servers were not actually used as “backup” servers for load balancing.

- Several inconsistencies in the configuration system had led to a few parameters having missing names, descriptions, suggestions, or unexpected behavior. These problems have been corrected.
- When the system was under heavy load, several noisy stack traces would be produced in the log file.
- When updating the system hostname via CLI, or when changing cluster membership, the Web UI would, in various locations, incorrectly display the old hostnames indefinitely, in addition to the current names.
- On High Availability deployments, attempting to use the VIP to set up SSL would not work.
- Passwords for external services, such as SMTP servers and backup FTP or SSH servers, were previously stored in plain text, allowing an attacker who obtained a configuration backup to view them. These values have been encrypted. Users who had these values set must re-set them after upgrading to 5.5.
- Under certain circumstances, a small memory leak would appear in the code handling database connections. This has been fixed.
- HTTP 400 Status Codes returned from a backend server would be incorrectly and silently converted into HTTP 503 Status Codes when the response passed through WebApp Secure.
- Under circumstances when a backend server returned a non-standard character set encoding, an HTTP 500 error was returned to the client
- System and security alerts were not sent consistently on SMTP servers that required authentication.
- System and security alerts were not sent consistently when the severity of the alert was below a certain threshold.
- Log rotation would only happen once per day, regardless of the log file size.
- Log rotation did not affect all log files, leading to a possibility of the disk filling up.
- Under certain circumstances, it was not possible to send a "Support bundle" on the secondary HA node.
- The graphs present on the Dashboard of the Web UI displayed incorrect timestamps when a user set a preferred timezone in their User Preferences, and filtered the display of information to "Last Day."

Known Issues

- Customers using the Autoresponse API to create custom Autoresponse rules should be aware that:
 - The "description" attribute is no longer exposed on the "incidentType" object

- The “uniqueid” attribute exposed on the “profile” object differs from the unique ID present in the full details of the response
- When using the “Search” functionality present in the HTML Administrator Guide, attempts to open search results in a new browser tab or window will result in an HTTP 404 error. Opening search results in the same tab or window works fine.
- In high availability deployments, after setting the Management VIP, you are directed to run the **set master-address <ip>** command. This assumes that you are in the CLI. If you are running CLI commands at the bash prompt, you will need to prefix this command with **cli system**. For example, **cli system set master-address <ip>**.
- In any tab of the Web UI that displays deployed counter responses, clicking the **Deactivate Selected** button with no responses selected, will result in a confusing error message.
- Only the first instance of a security incident for a given session will result in an entry in the security alert log. Repeated instances of the same incident will not print to the log.
- The CLI shows “RAID Status” as an available option, regardless of deployment type. The RAID Status option is only available on hardware / High Availability deployments.
- If you perform a configuration export through the configuration CLI, make changes to the configuration through the Web UI, and then attempt to import the configuration through the CLI without first exiting and re-entering the CLI, you may encounter an error upon import.
- WebApp Secure 5.5 is vulnerable to OpenSSL CVE-2014-0076, which enables a local attacker to obtain ECDSA nonces via a side-channel attack. It is recommended that console access to WebApp Secure be limited, which should mitigate the risk. There are no known ways to exploit this vulnerability remotely.
- When unsetting network interface aliases through the CLI, the Linux networking module will remove the routes associated to the interface, effectively severing all connections to the main interface. While it might appear that the parent interface (the interface from which the alias was created as a part of) is gone, simply restarting networking via the console using the CLI command **cli system services restart network** should re-create the routes to the interface and put the system in a working state again.
- In the system networking config (cli system interfaces), you can set the interface boot type to be DHCP. However, you can also set it to have an IPADDR, NETMASK, and GATEWAY. A quick glance at this configuration, and you would expect the system to have the IP listed there. However, DHCP has a higher precedence and overrides the IP settings. Thus, the actual IP address will be completely different. While this works as designed, it nonetheless is confusing to look at.

Requesting Technical Support

To open a case or to obtain support information, please visit the Juniper Networks Support Site: <http://www.juniper.net/support>

WebApp Secure Documentation and Release Notes

For a list of related WebApp Secure documentation, see the [WebApp Secure Documentation](#) section of the Juniper web site.

To obtain the most current version of all Juniper Networks technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.