WebApp Secure 5.6 Release Notes Release Notes

Release 5.6
January 2015
Revision 1

These release notes accompany Release 5.6 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 5.6 Release Overview

The 5.6 release contains two important features, one related to easy deployment with the SRX series and another called “Silent Running” mode which allows the effects of counter-responses deployed on an attacker to be silenced without impacting monitoring and reporting functionality. The release has a number of other operational and UI improvements as well as bug fixes aimed at improving the following:

- Deployment
- Security
- Supportability

New and Changed Features

- Deploy with SRX

  You can easily deploy WebApp Secure behind your SRX series with a simple push of a button, utilizing OSPF or BGP routing. Routing changes take effect dynamically and route traffic to WebApp Secure or to the original destination in case of a failure.

- Silent Running Mode

  Silent Running Mode allows the effects of counter-responses deployed on an attacker to be silenced, without impacting monitoring and reporting functionality. When Silent Running is enabled, the Web UI and reports display that counter responses have been activated, but the counter responses are not actually be deployed on site to users. This allows WebApp Secure to be used for monitoring and reporting, but not enforcement.

- Other Improvements
  - Self-service evaluation license form built-in to WebApp Secure allows for simpler proof-of-concept deployment by allowing customers to request their own evaluation licenses without the need to contact Juniper support.
  - SSL ciphers and protocols may now be configured on a per-application basis. If not configured, they will default to the new, secure values introduced in the 5.5 release.
  - The HTTP version used for proxying can now be configured. While HTTP 1.0 is still the default, and suitable for most deployments, customers may now choose to use HTTP 1.1 instead.
  - Autoresponse rules may now be cloned and customized. Additionally, the syntax used for these rules has been simplified and re-documented. Autoresponse rules control the main counter-response functionality of WebApp Secure, and the ability to customize them has been requested by numerous customers.
  - The Spotlight Secure Cloud Service has been integrated into the system alerts functionality introduced in 5.5.0. Additionally, it is now turned on by default for new installations of WebApp Secure 5.6. If you are upgrading an existing system, your current settings will not be changed.

- When configuring listening IP addresses for an application, the Web UI now shows the host and interface for the given IP addresses in the list, simplifying configuration in cluster or high-availability deployments.
- Tables of data in the Web UI are now "fluid". Columns will intelligently show/hide themselves based on the width of the browser viewport.
- Added "Test These Settings" buttons in Web UI for health check parameters, backend servers, and LDAP servers. These buttons help prevent problems caused by invalid configuration.
- Minor tweaks to the visual style and consistency of the Web UI.
- New layout and graphs for attackers, sessions, and incidents landing pages.
- NTP Server configuration has been added to the Web UI's first-run wizard.
- The WebApp Secure Support Bundle, a collection of system information often requested by JTAC or Engineering for troubleshooting purposes, can now be generated and manually exported. Previously, this functionality required outbound HTTPS access to the WebApp Secure licensing system, which was not possible for all deployments.

Installation and Deployment Notes

- Please note that WebApp Secure 5.6 requires a reboot after the update completes.
- It is highly recommended that you consult the Release Notes for WebApp Secure 5.5.0 before attempting any upgrades. The release notes are available here on the Juniper web site.
- 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 5.1.x, please upgrade to 5.1.3-32 first. Then follow the instructions for release 5.5 provided here.

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

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.

- [PR 1025219] Fixed an issue with old Web UI sessions filling up the disk over time
- [PR 1026167] Fixed an issue that caused configuration corruption when choosing specific options in the File Processor
- [PR 1029363] Applied security patch for CVE-2014-6271 and CVE-2014-7169
- [PR 1038147] Updated “Test SMTP Connection Settings” to use “SMTP Server Timeout” value
- Disabled WebUI service on non-management interfaces
- Prevent URL Fuzzing false positives when non-standard TLDs are used
- Fixed issue preventing some configuration "suggestions" from being used in the CLI
- Numerous small documentation inconsistencies were resolved
- Numerous small configuration system validators were added, further ensuring that only valid configuration gets saved
- Further enhancements to new HTML manipulation engine introduced in 5.5 release to address minor bugs found in edge cases
- CLI no longer incorrectly shows RAID status on non-hardware deployments

Known Issues

- After upgrading the appliance, under certain circumstances, you may notice a large stack trace in mws.log related to the Request Captcha Processor. To stop these errors from occurring, run the following commands in the WebAppSecure bash shell:

  cli config set services.response.silent.enabled false

- WebApp Secure 5.6 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.
- After the update is completed, following error message is shown. However, the system continues to function normally.

  Oct 3 17:48:10 test1003offline [mws-pyro][INFO] Complete!

  Oct 3 17:48:11 test1003offline [mws-config][ERROR] ConfigurationManager instance has no attribute 'affected_parameters'

  Traceback (most recent call last):

File "/usr/lib/python2.6/site-packages/Mykonos/Config/Manager.py", line 1284, in _run_handlers"

- In rare circumstance, when the backend server sends a header larger than 4K, the following message will appear in the access.log **jwas proxy: [error] 10772#0: *117181 upstream sent too big header while reading response header from upstream**. The end user would see a "502 Bad Gateway" in such cases. There is a workaround for this that requires a support call to WebApp Secure engineering.

Requesting Technical Support

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

For additional information about WebApp Secure, please refer to the WebApp Secure Administrator Guide and WebApp Secure Developer Guide available from the “Help” section of the Web UI.

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/.