WebApp Secure 5.1.3-30

Release Notes: (April 10, 2014)

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

April, 2014

Contents

For additional information about WebApp Secure, please refer to the *WebApp Secure Administrator Guide and WebApp Secure Developer Guide.*

Synopsis

5.1.3-30 Maintenance release contains an updated OpenSSL library to resolve CVE-2014-0160, known as the "Heartbleed" vulnerability. Additionally, 5.1.3-30 contains 3 other bug fixes, discussed in the “Bug Fixes” section below. 5.1.3-30 includes all the changes made in the previous releases 5.1.3-4 and 5.1.3-24. If you would like to learn more about feature updates and bug fixes in those releases please review the respective release notes at http://www.juniper.net/support/downloads/?p=jwas#docs”.

This release is only available as a .tar file update.

Installation and Deployment

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 to 5.1.3-30 then after the upgrade, **WebApp Secure system requires a reboot** due to a change in the Linux Kernel.

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

Documentation is available at http://www.juniper.net/support/downloads/?p=jwas#docs

Bug Fixes

- OpenSSL library is updated to a recently patched version “openssl-1.0.1e-16.el6_5.7.x86_64” that does not have Heartbleed vulnerability (CVE-2014-0160).

  It is recommended that you restart nginx after the update to ensure if your system had the old library then it is not being used any longer; the command to do so is “sudo /etc/init.d/nginx restart”. NOTE: This will briefly interrupt access to your website during the nginx restart.
- WebApp Secure was incorrectly sending a 503 status code when the actual backend application was returning a 400 status code. The correct result is to pass forward the 400 status code to the client.
- [PR 971594, JTAC Case ID:2014-0304-1399] Any incident of "informational" or "suspicious" severity was not getting logged in unless incident could be associated to an existing profile.
- Blank google map is displayed on accessing the web application even if 'Google Map' response is activated for a malicious profile. Google deprecated an API used by WebApp Secure on the client side code; the release now uses new Google API.

Known Issues and Limitations

- Please note that all the Known issues and Limitations noted for release 5.1.3-4 and 5.1.3-24 also apply to 5.1.3-30 as this release fixes 3 bugs and does not provide any other enhancements.

Requesting Technical Support

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