EZproxy 7.1.14 release notes, March 2021

Release Date: March 23, 2021

Overview

EZproxy v7.1.14 is a maintenance release building on EZproxy v7.1, one of our biggest releases to date. EZproxy v7.1.14 fixes several bugs that were introduced in v7.1 and includes an OpenSSL update to provide best-in-class security.

Supporting materials

- Software download
- Product Insights
- Upgrade guide
- EZproxy v7.1 release notes

Improvements and bug fixes

1. EZproxy v7.1.14 was built with OpenSSL 1.1.1j (released 16 February 2021). This update addressed one vulnerability of moderate severity and one of low severity.

2. The previously released version of EZproxy v7.1 for Linux, when started as root with RunAs in config.txt, created the security directory as the root user. If the pseudonymous identifier feature was enabled, the identifier database was also created as the root user. The code has been changed to create the security directory and the identifier database under the RunAs user, not under root.

   • Upgrade note: This applies only to sites that have already upgraded to the previously released version of EZproxy v7.1 for Linux AND are starting the software as root with RunAs in config.txt. These sites may have the security directory and/or files contained in the security directory owned by root. In these cases, you will need to manually change the ownership of these files to match the RunAs user if they are owned by root.

3. The previously released version of EZproxy v7.1 froze when setting session variables, which are normally set in user.txt or shibuser.txt. This has been corrected.

4. The previously released version of EZproxy v7.1, if the pseudonymous identifier feature was disabled, froze during the identifier and security database purges. This has been corrected.
Known issues

1. Potential rules trip if the site uses SAML authentication and usernames are not set in shibuser.txt.

If the EZproxy session variables, login:loguser and login:user, are not set in shibuser.txt, then the default username for all users using SAML authentication becomes “shibboleth.” In this case, since groups are tripped at the username level, false trips of rules may occur.

2. Rules with longer watch periods will consume more disk space to store evidence.

Increasing the watch period from 60 minutes or longer will consume more disk space in the /security directory to store the required evidence in the security database. Please monitor the disk usage in the /security database.

Some of the default rules shipped in EZproxy 7.1 contain monitoring periods longer than 60 minutes. If you find you are having disk space constraints, consider commenting out those rules or shortening the monitoring periods.