PROXEDO

API SECURITY

Proxedo API Security

Release notes for PAS 4.5.0

DISCLAIMER

Balasys is not responsible for any third-party websites mentioned in this document. Balasys does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. Balasys will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

2023-07-20

The following new features, bug fixes and improvements have been completed for Release 4.5.0 Proxedo API Security.

Features

- **WAF Enforcer**
  To complement the positive security model enforcement capabilities, PAS now features a Web Application Firewall module that provides rule-based attack prevention and virtual patching for known web-based security vulnerabilities. The WAF Enforcer protects against a variety of application layer attacks including credential theft, code injection, cross-site scripting (XSS), cookie poisoning, CSRF, SQL injection, DoS, ransomware, and more. The WAF Enforcer is built on top of the proven ModSecurity open-source web security framework. The use of the WAF Enforcer is subject to a separate license, please contact our sales team at sales@balasys.hu for pricing and further details.

Bug Fixes

- **Miscellaneous fixes**
  - When encountering an error during upgrading the configuration, the post-upgrade phase of the pas-mgmt-upgrade-config tool only displayed a generic error message. This has been improved to provide additional details of the error.
  - The Elasticsearch Insight target encountered an error while sending Insights. This has been corrected.

Improvements

- **Elasticsearch Insight targets use bulk inserts**
  PAS now uses bulk inserts when sending Insights to an Elasticsearch target. This improves Elasticsearch performance when handling large traffic volumes.
- **Ephemeral storage settings for Kubernetes deploments**
  PAS now support requests and limits for ephemeral storage when deployed in Kubernetes.
- **Separate resource limits for Kubernetes deploments**
  PAS only supported resource limits that define both CPU and memory limits when deployed in Kubernetes. These limits can now be defined separately as well.

Notable changes

- **Elasticsearch Insight targets do not need doc_type defined**
  PAS now does not need a document type defined for its Elasticsearch Insight targets. The default document type parameter was deprecated with Elasticsearch 6.