СПРАВКА

о результатах автоматизированной проверки уязвимостей в сервисах релиза 1.12.0.

В рамках подготовки релиза 1.12.0 была выполнена автоматизированная проверка контейнерных образов следующих сервисов:

- idm-v3
- idm-v2

Проверка осуществлялась с использованием инструмента анализа уязвимостей Trivy версии 0.61.0. В процессе сканирования анализировались потенциальные уязвимости в:

- базовых образах (операционная система и системные пакеты);
- зависимостях приложений (библиотеки и компоненты).

Отчёт сформирован на основе данных, актуальных на момент анализа (31.07.2025), учитывая встроенную базу известных уязвимостей Trivy.

Детализированные результаты приведены в Приложении 1.

Начальник отдела безопасной разработки А.В. Новиков

Директор департамента ИБ Д.В. Абраменко

Директор департамента производства Н.С. Данковцева

Приложение 1.

Наименование сервиса	**Уровень критичности**	**CVE**	**Наименования компонента**	**Установленная версия компонента**	**Версия компонента для исправления**	**Обоснование**
idm-v3	Уязвимостей в образе не выявлено					
idm-v2	High	CVE-2024-2398	curl	8.5.0-r0	8.7.1-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-6197	curl	8.5.0-r0	8.9.0-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-6119	libcrypto3	3.1.4-r1	3.1.7-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-2398	libcurl	8.5.0-r0	8.7.1-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-6197	libcurl	8.5.0-r0	8.9.0-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.

	High	CVE-2024-6119	libssl3	3.1.4-r1	3.1.7-r0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2025-48734	commons-beanutils:commons-beanutils	1.9.4	1.11.0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-47554	commons-io:commons-io	2.8.0	2.14.0	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.
	High	CVE-2024-51504	org.apache.zookeeper:zookeeper	3.9.2	3.9.3	На уровне кода исключены условия, позволяющие реализовать выявленные уязвимости, которые описаны в базе данные уязвимостей NVD.