

???????? SUID-SGID ?????? ? ?????? ?????????? ???????????

Зона ответственности: Printum

Коротко: Контейнерные образы Printum не содержат файлов с установленными битами SUID/SGID и не включают утилиты повышения привилегий, позволяющие получить дополнительные права внутри контейнера.

??????????

Контейнерные образы не должны содержать механизмы, позволяющие повысить привилегии процесса или пользователя внутри контейнера.

Удаление SUID/SGID-файлов и утилит повышения привилегий снижает риск несанкционированного получения дополнительных полномочий при компрометации контейнера.

??? ??? ?????????????? ? Printum

При сборке производственных контейнерных образов Printum выполняется удаление файлов с установленными битами SUID и SGID.

Аналогичная обработка применяется для основных компонентов системы:

- Мониторинг;
- ПринтМенеджер;
- File Server ПринтМенеджера;
- CUPS.

Дополнительно из образов удаляются утилиты повышения привилегий, включая su.

Такой подход исключает использование механизмов повышения привилегий через SUID/SGID-бинарники и ограничивает возможности получения дополнительных прав внутри контейнера.

Удаление выполняется на этапе сборки образов и входит в стандартный процесс подготовки production-версий контейнеров.

??? ?????????????? Printum

Printum обеспечивает:

- отсутствие файлов с установленными битами SUID и SGID в производственных образах;
 - отсутствие утилит повышения привилегий;
 - соответствие принципу минимально необходимых привилегий для контейнерных компонентов.
-