Внешнее ревью

example.org

Учебный пример · синтетические данные / 2026-11-22 / Частичное покрытие

Источники · внешние измерения HTTP/TLS, DNS, предоставленный инженером XML Nmap, локальный каталог бюллетеней MariaDB

01 Краткий вывод

Первым разберите наблюдение E005. MariaDB · 192.0.2.42:44332/tcp.

02 Наблюдаемая поверхность

Показано 5 из 5 записей. Всего доказательств: 8.

E005 192.0.2.42:44332/tcp · MariaDB 10.11.8-MariaDB-0+deb12u1 (Nmap XML)

E004 192.0.2.42:10051/tcp · служба не установлена

E006 192.0.2.42:9443/tcp · Management console

E007 192.0.2.42:53/udp · open|filtered · состояние неопределённо

E008 https://example.org/ · HTTP 200

03 Приоритетные наблюдения

E005 MariaDB · 192.0.2.42:44332/tcp

Доступность службы · Сеть допускает соединение с интерфейсом службы. Требования к авторизации и права доступа неизвестны.

E006 Management console · 192.0.2.42:9443/tcp

Доступность службы · Сеть допускает соединение с интерфейсом службы. Требования к авторизации и права доступа неизвестны.

Приоритетных наблюдений: 4. Все доказательства и рекомендации доступны в закрытом HTML.

04 Оценка HTTP-заголовков КУБИТ

E008 https://example.org/ · 3 из 6 критериев

Один балл за каждый выполненный применимый критерий. На HTTPS оценивается HSTS от одного года. Для успешного ответа учитывается nosniff. Для HTML дополнительно оцениваются ограничения скриптов, встраивания, передачи Referer и отключение чувствительных возможностей браузера. Report-Only и атрибуты cookie приводятся справочно.

KUBIT-HTTP/1.0

05 Версии и CVE

Дата анализа · 2026-11-22

Кандидаты по версии: 2. E005 · CVE-2026-107816. Применимость требует проверки. Источники в HTML.

06 Границы проверки

DNS · завершено 2, частично 0, ошибок 0, пропущено 0.
HTTP/TLS · завершено 1, частично 0, ошибок 0, пропущено 0.
Адресов в XML Nmap: 1. Неполные сведения: 1.
E001 · PTR не получен. Другие записи рассматривались отдельно.

E003 · 192.0.2.42 · В XML отсутствует отметка об успешном завершении запуска.

Проверка веба ограничена исходным именем, стандартными HTTP/HTTPS и выбранными публичными адресами.

Поиск TCP-портов и UDP: not_run. Перечень соседних сайтов на IP неизвестен.

CT, passive DNS и NVD не запрашивались. Применимость CVE требует отдельной проверки.

07 Следующие действия

1. Сверить назначение точки входа и разрешённые сети доступа.
2. Проверить отмеченные критерии на этом URL перед изменением политики.
3. Согласовать с владельцем адресов границы следующей проверки.
4. Сверить сообщённые версии со сборками и уведомлениями поставщика.

08 Назначение и ограничения

BLACKBOX помогает владельцам инфраструктуры и уполномоченным специалистам определить приоритетные меры по повышению её защищённости.

Отчёт составлен по следующим источникам в пределах указанного покрытия: внешние измерения HTTP/TLS, DNS, предоставленный инженером XML Nmap, локальный каталог бюллетеней MariaDB.

Рекомендации предназначены для устранения выявленных недостатков конфигурации и проверки потенциальных рисков.

Сопоставление продукта и версии с CVE указывает на возможную применимость уязвимости и требует проверки конкретной сборки, конфигурации и установленных исправлений.

Эксплуатация уязвимостей не выполнялась. Отчёт отражает состояние на момент измерений; отсутствие находок не гарантирует отсутствие уязвимостей.

09 Доказательства и источники

E005 · MariaDB · 192.0.2.42:44332/tcp
Сверить назначение точки входа и разрешённые сети доступа.

E006 · Management console · 192.0.2.42:9443/tcp
Сверить назначение точки входа и разрешённые сети доступа.

E005 · CVE-2026-107816 · 192.0.2.42:44332/tcp
https://github.com/MariaDB/server/security/advisories/GHSA-wfqg-88r5-55f6

В закрытом HTML доступны подробные наблюдения и основания выводов по каждому номеру доказательства.