НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200506.8| 6 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в ОС Red Hat Enterprise Linux 7

Идентификатор уязвимости	MITRE: CVE-2019-13734
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Уязвимость позволяет удаленному злоумышленнику выполнять произвольный код в целевой системе посредством отправки специально сформированных данных в уязвимое приложение. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных в ядре базы SQLite.
Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимое ПО	Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.6 s390x Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.6 ppc64 Red Hat Enterprise Linux EUS Compute Node 7.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.6 ppc64le Red Hat Enterprise Linux Server - TUS 7.6 x86_64 Red Hat Enterprise Linux for ARM 64 7 aarch64 Red Hat Enterprise Linux for Power 9 7 ppc64le Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.6 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 7.6 x86_64 Red Hat Enterprise Linux for IBM System z (Structure A) 7 s390x

Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 мая 2020 г.
Дата обновления	5 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://access.redhat.com/errata/RHSA-2020:2014 https://www.cybersecurity-help.cz/vdb/cvss3/#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C