

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220727.21 | 27 июля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольных SQL-запросов в Red Hat Update Infrastructure (RHUI)

Идентификатор уязвимости	MITRE: CVE-2022-28346 CVE-2022-28347
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Red Hat Update Infrastructure (RHUI): 4.1.0 python-future (Red Hat package): 0.18.2-4.el8pc python-django (Red Hat package): 3.2.13-1.el8pc python-cryptography (Red Hat package): 3.1.1-1.el8pc pulpcore-selinux (Red Hat package): 1.3.0-1.el8pc createrepo_c (Red Hat package): 0.20.0-1.el8pc rhui-tools (Red Hat package): до 4.1.1.16-1.el8ui rhui-installer (Red Hat package): до 4.1.1.8-1.el8ui rhui-cds-plugin-fetcher (Red Hat package): до 1.0.5-1.el8ui rhui-cds-plugin-authorizer-cert (Red Hat package): до 1.0.5-1.el8ui python-url-normalize (Red Hat package): до 1.4.3-4.el8ui python-requests (Red Hat package): до 2.27.1-2.el8ui python-pyjwt (Red Hat package): до 1.7.1-8.el8ui python-pyjwtkest (Red Hat package): до 1.4.2-6.el8ui python-псcryptodomex (Red Hat package): до 3.14.1-2.el8ui python-pyOpenSSL (Red Hat package): до 19.1.0-3.el8ui

	<p>python-pulpcore (Red Hat package): до 3.17.6-3.el8ui</p> <p>python-pulp-rpm (Red Hat package): до 3.17.5-2.el8ui</p> <p>python-pulp-container-client (Red Hat package): до 2.7.1-6.el8ui</p> <p>python-pulp-container (Red Hat package): до 2.10.3-2.el8ui</p> <p>python-ecdsa (Red Hat package): до 0.14.1-2.el8ui</p> <p>ansible-collection-community-crypto (Red Hat package): до 1.7.0-4.el8ui</p>
Рекомендации по устранению	<p>Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>
Дата выявления	19 июля 2022 г.
Дата обновления	19 июля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://access.redhat.com/errata/RHSA-2022:5602