

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: gov-cert@gov-cert.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190704.4 | 4 июля 2019 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Переполнение буфера в ПО Qemu

Идентификатор уязвимости	MITRE: CVE-2018-20815
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством переполнения буфера функции <code>load_image</code> в <code>device_tree.c</code> .
Уязвимое ПО	Qemu включая v3.1.0
Рекомендации по устранению	Обновить программное обеспечение
Дата и время выявления	31 мая 2019 г.
Дата и время обновления	2 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O
Вектор атаки	Сетевой
Сложность эксплуатации уязвимости	Низкая
Требуемый уровень привилегий	Отсутствует
Взаимодействие с пользователем	Не требуется
Влияние на другие компоненты системы	Не оказывает
Наличие эксплоита	Демонстрация возможности
Средство устранения уязвимости	Официальное решение
Ссылки на источники	https://access.redhat.com/errata/RHSA-2019:1667 https://git.qemu.org/?p=qemu.git;a=commitdiff;h=da885fe1ee8b4589047484bd7fa05a4905b52b17