НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190829.1 | 29 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Переполнение буфера в ПО SLiRP эмулятора QEMU

Идентификатор уязвимости	MITRE: CVE-2019-14378
Идентификатор программной ошибки	CWE-122: Переполнение буфера на основе кучи
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании посредством запуска вредоносного файла. Уязвимость обусловлена переполнением буфера функции ip_reass в файле ip_input.c.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	QEMU до v0.2.2, v0.3.1, v0.4.0-beta.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 июля 2019 г.
Дата обновления	10 августа 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.0 AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:H/E:F/RL:O/RC:C
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Не требуется (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Низкое (L)

Влияние на целостность (I)	Низкое (L)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Функциональная версия (F)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://access.redhat.com/security/cve/cve-2019-14378 https://gitlab.freedesktop.org/slirp/libslirp/commit/126c04acbabd7ad32c2b018fe10dfac2a3bc1210 https://github.com/vishnudevtj/exploits/tree/master/qemu/CVE-2019-14378 https://github.com/rootless-containers/slirp4netns/security/advisories/GHSA-gjwp-vf65-3jqf