НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200326.5 | 26 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в менеджере пакетов OPKG в OpenWrt

Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимое ПО	OpenWrt: 18.06.0, 18.06.1, 18.06.2, 18.06.3, 18.06.4, 18.06.5, 18.06.6, 19.07.0 LEDE: 17.01.0, 17.01.1, 17.01.2, 17.01.3, 17.01.4, 17.01.5, 17.01.6, 17.01.7
Дата выявления	25 марта 2020 г.
Дата обновления	25 марта 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-7982	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством применения атаки «человек посередине» и внедрения вредоносных пакетов данных. Уязвимость обусловлена некорректной проверкой целостности загруженных пакетов с использованием контрольных сумм SHA-256 в диспетчере пакетов OPKG. CVSS:3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-74: Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение) Рекомендации по устранению: Обновить программное обеспечение.	9,8

MITRE: CVE-2020-7248	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке больших двоичных объектов в библиотеке libubox. 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 CWE-787: Запись за границами буфера Рекомендации по устранению: Обновить программное обеспечение.	9,8

Ссылки на источники	https://blog.forallsecure.com/uncovering-openwrt-remote-code-execution-cve-2020-7982 https://openwrt.org/advisory/2020-01-31-1 https://openwrt.org/advisory/2020-01-31-2 https://www.cybersecurity-help.cz/vdb/SB2020032508