НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200520.2 | 20 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в FreeRDP

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	FreeRDP до v2.0.0-rc4
Дата выявления	15 мая 2020 г.
Дата обновления	15 мая 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2019-17177	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена утечкой памяти в libfreerdp/codec/region.c. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-190: Некорректное освобождение памяти до удаления последней ссылки (Утечка памяти) Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-11521	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством использования специально сформированных вредоносных данных. Уязвимость обусловлена возможностью записи данных за пределы буфера памяти в libfreerdp/codec/planar.c CVSSv3.0: 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
MITRE: CVE-2020-11522	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным или вызвать отказ в обслуживании целевой системы посредством использования специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ буфера памяти в libfreerdp/gdi/gdi.c. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	8.1
MITRE: CVE-2020-11525	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным посредством использования специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ буфера памяти в libfreerdp/cache/bitmap.c. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2020-11526	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством использования специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ буфера памяти в функции update_recv_secondary_order в файле libfreerdp/core/update.c. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://security.gentoo.org/glsa/202005-07 https://www.cybersecurity-help.cz/vdb/SB2020051818