НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200518.6 | 18 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-2020-11523	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена целочисленным переполнением буфера памяти в libfreerdp/gdi/region.c. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2020-11524	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/gdi/interleaved.c. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение.	9.8

Ссылки на источники	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4qrh-8cp8-4x42 https://nvd.nist.gov/vuln/detail/CVE-2020-11523 https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-cgw8-3mp2-p5qw https://nvd.nist.gov/vuln/detail/CVE-2020-11524 https://www.cybersecurity-help.cz/vdb/SB2020051817