НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200605.6 | 5 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО Zoom

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Zoom Client Application v4.6.10, v4.6.11
Дата выявления	3 июня 2020 г.
Дата обновления	3 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-6109	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сообщения в чат уязвимого приложения. Уязвимость обусловлена некорректной работой расширения для поддержки анимированных GIF-сообщений при загрузке файлов с сервиса Giphy. CVSSv3.0: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	8.5

MITRE: CVE-2020-6110	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного zip-архива, используя функцию отправки фрагментов кода в уязвимом приложении. Уязвимость обусловлена некорректной проверкой файлов перед извлечением из zip-архива в клиенте Zoom. CVSSv3.0: AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	8.0

Ссылки на источники	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1056