НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200415.3| 15 апреля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО Microsoft Excel

Идентификатор уязвимости	MITRE: CVE-2020-0906 CVE-2020-0979
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректным определением границ буфера памяти в ПО Microsoft Excel.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Microsoft Office: 365 ProPlus, 2010 SP 2, 2013, 2013 RT, 2016, 2019 Microsoft Excel: 2010, 2013, 2013 RT SP 1, 2016
Рекомендации по устранению	Обновить программное обеспечение
Датавыявления	14 апреля 2020 г.
Датаобновления	14 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.7 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0906 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0979 https://www.cybersecurity-help.cz/vdb/SB2020041417