НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200616.2| 16 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Microsoft VBScript

Идентификатор уязвимости	MITRE: CVE-2020-1213 CVE-2020-1214 CVE-2020-1215 CVE-2020-1216 CVE-2020-1230 CVE-2020-1260
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимостей позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла или веб-страницы. Уязвимость обусловлена некорректной обработкой объектов в памяти механизма VBScript.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Microsoft Internet Explorer 11 Microsoft Internet Explorer 9
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 июня 2020 г.
Дата обновления	9 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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-2020-1213 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1214 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1215 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1216 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1230 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1260