НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191224.4 | 24 декабря 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в веб-браузере Microsoft Internet Explorer

Идентификатор уязвимости	MITRE: CVE-2019-1429
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному не аутентифицированному злоумышленнику выполнять произвольный код в целевой системе с правами текущего пользователя посредством открытия пользователем вредоносного сайта или специально созданного документа. Уязвимость обусловлена некорректной работой обработчика сценариев.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Internet Explorer 9 для: Windows Server 2008 x32/x64 SP 2 Internet Explorer 10 для: Windows Server 2012 Internet Explorer 11 для: Windows 10 Version 1803 x32/x64/ARM64 Windows 10 Version 1809 x32/x64/ARM64 Windows 10 Version 1709 x32/x64/ARM64 Windows 10 Version 1903 x32/x64/ARM64 Windows 10 x32/x64 Windows 10 Version 1607 x32/x64 Windows 7 x32/x64 SP 1 Windows 8.1 x32/x64 Windows RT 8.1 Windows Server 2008 R2 for x64-based Systems SP 1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019

Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 ноября 2019 г.
Дата обновления	21 ноября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2019-1429 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429 https://www.securitylab.ru/vulnerability/502478.php