

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200818.1 | 18 августа 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в Internet Explorer

Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Internet Explorer 9, 11
Дата выявления	11 августа 2020 г.
Дата обновления	11 августа 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-1380	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями текущего пользователя в целевой системе посредством открытия пользователем специально созданных вредоносных веб-страницы или документа Microsoft Office. Уязвимость обусловлена некорректным способом обработки сценариев объектов памяти в Internet Explorer.</p> <p>CVSSv3.1: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5

MITRE: CVE-2020-1567	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями текущего пользователя в целевой системе посредством редактирования пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных механизмом MSHTML.</p> <p>CVSSv3.1: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	7.5
Ссылки на источники	<p><a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2020081114">https://www.cybersecurity-help.cz/vdb/SB2020081114</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1567">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1567</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2020081230">https://www.cybersecurity-help.cz/vdb/SB2020081230</a></p>	