

# 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 УЯЗВИМОСТИ

VULN-20200615.4 | 15 июня 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Microsoft SharePoint

Идентификатор уязвимости	MITRE: CVE-2020-1181
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством загрузки специально сформированного вредоносного XML-файла при создании страницы SharePoint. Уязвимость обусловлена некорректной обработкой веб-элементов управления ASP.Net в Microsoft SharePoint.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимое ПО	Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Foundation 2010 SP2 Microsoft SharePoint Foundation 2013 SP1 Microsoft SharePoint Server 2019
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 июня 2020 г.
Дата обновления	9 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

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	<a href="https://www.zerodayinitiative.com/advisories/ZDI-20-694/">https://www.zerodayinitiative.com/advisories/ZDI-20-694/</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1181">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1181</a>