НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Выполнение произвольного кода в Microsoft MSHTML

CVE-2021-40444

ALRT-20210910.1 | 10 сентября 2021 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Уязвимое программное обеспечение	Microsoft Windows 7, 8.1, 10 Microsoft Windows Server 2008, 2012, 2016, 2019, 2022
Описание угрозы	Эксплуатация уязвимости в Microsoft MSHTML позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного документа Microsoft Office. Уязвимость обусловлена некорректной проверкой входных данных в компоненте MSHTML. Официальное исправление указанной уязвимости в настоящее время отсутствует. По имеющимся сведениям, злоумышленники начали активно использовать данную уязвимость в целевых компьютерных атаках при внедрении различного ВПО. В ходе таких атак ими используются методы социальной инженерии с целью убеждения пользователей открыть зараженный документ Microsoft Office, вследствие чего происходит эксплуатация указанной уязвимости и загрузка полезной нагрузки ВПО. Отмечаем, что с учетом повышенного интереса злоумышленников к указанной уязвимости и отсутствия официальных исправлений от компании Microsoft создаются предпосылки для массового заражения пользователей различным ВПО. В настоящее время имеются факты о доставке таким образом ВПО Cobalt Strike. Бюллетень НКЦКИ об указанной уязвимости опубликован по следующей ссылке: https://safe-surf.ru/upload/VULN/VULN-20210908.5.pdf
Рекомендации по нейтрализации угрозы	В целях нейтрализации данной угрозы рекомендуем: 1. Воспользоваться временным решением компании Microsoft по отключению возможности установки ActiveX компонентов в ОС и отключения предварительного просмотра документов в Windows Explorer. Подробная инструкция описана в разделе Workarounds по следующей ссылке https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444 2. Обновить используемые антивирусные средства. 3. Проверить на ресурсах ИТС и в сетевом трафике наличие индикаторов компрометации, представленных в файле «IOC.csv».

	4. Провести мероприятия, нацеленные на повышение бдительности и осведомленности сотрудников Вашей компании в части противодействия фишинговым атакам и иным методам социальной инженерии. 5. При получении электронных писем с приложенным файлами производить их проверку антивирусными средствами или средствами динамического анализа. В случае выявления признаков компрометации ИТС Вашей компании просим сообщить об этом в НКЦКИ.
Ссылки на источники	https://www.securitylab.ru/vulnerability/524175.php https://www.cybersecurity-help.cz/vdb/SB2021090712 https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0821_CVE0DAy https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444