НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20201223.4 | 23 декабря 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО Foxit Reader

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Foxit Reader v10.1.0.37527
Дата выявления	9 декабря 2020 г.
Дата обновления	9 декабря 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-13557 CVE-2020-13560	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла или веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в движке JavaScript. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.8

MITRE: CVE-2020-13547	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена использованием несовместимых типов в функции openPlayer(). CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов) Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2020-13548	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла или веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в движке JavaScript. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.0
MITRE: CVE-2020-13570	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла или веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в движке JavaScript. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	7.5

Ссылки на источники	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1171 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1175 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1165 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1166 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1181