

Модуль 2. Построение системы защиты сети (HW)

Сканирование хоста на предмет уязвимости с помощью Scan OVAL

1. Проведите сканирование хоста или сети на наличие уязвимостей.

The screenshot shows the ScanOVAL application window. At the top, there are tabs for 'ScanOVAL' (highlighted in green), 'ГЛАВНОЕ' (Main), and 'СПРАВКА' (Help). Below the tabs, a status bar indicates '2 файла(ов) загружено.' (2 files loaded). The main area has a header with filters: 'Отображать:' dropdown set to 'Только обнаруженные' (Only detected), followed by four buttons: 'Результат' (Result), 'Уровень о...' (Level), 'Ссылки на источники' (Links to sources), and 'Название уязвимости' (Vulnerability name). A large table below shows the results grouped by severity level:

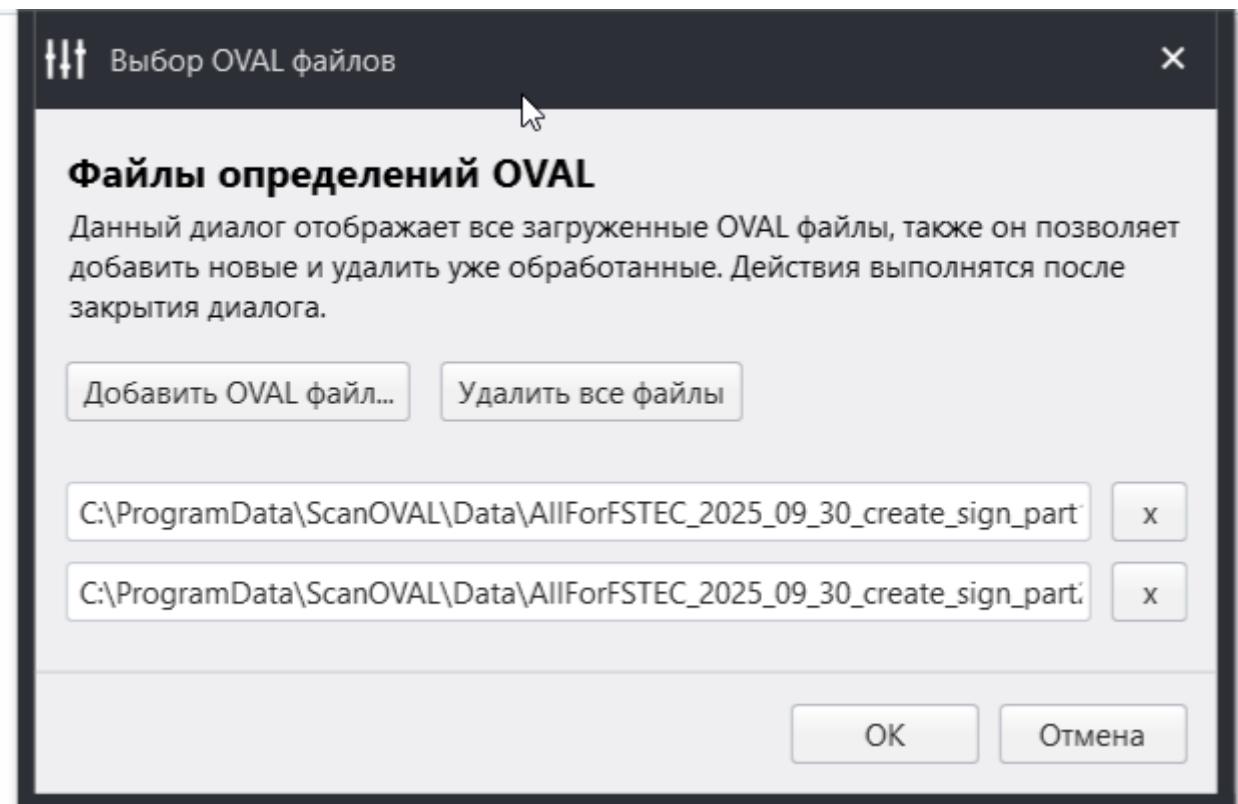
Критический (372)
Высокий (265)
Средний (255)
Низкий (23)

At the bottom of the table, there are buttons for 'Группировать по рискам' (Group by risk) and 'Группировать по продуктам' (Group by product), along with numerical counts: 372, 265, 255, 23. To the right, it says 'Всего: 915'. The footer of the window includes the text '© ФАУ «ГНИИИ ПТЗИ ФСТЭК России»'.

Не буду приводить развернутый список результата скана уязвимостей своего хоста. Результат сгруппирован по уровню уязвимости.

Критических - 372 Высоких - 265 Средних - 256 Низких - 25

В качестве базы уязвимостей использовались два файла определений с сайта
<https://bdu.fstec.ru/site/scanova>



2. Проанализируйте любую критическую уязвимость. Если критическая уязвимость отсутствует, то возьмите следующую по критичности.

Вот пример отчета, который был сгенерирован в html после проведения сканирования

ScanOVAL **ОТЧЕТ**

№ отчета	4c8a84f1-a03e-4897-a938-a7ff4f7033bf
№ сканирования	ac33878c-af60-40e5-945b-301a8a96fe6b
Профиль	Уязвимости
Начало/завершение сканирования	04.10.2025 11:46:17 / 04.10.2025 11:48:52
Формирование отчета	04.10.2025 12:12:47

Уровень опасности	Найдено	Всего
Критический	372	5701
Высокий	265	12439
Средний	255	12991
Низкий	23	1487
Недоступно	0	1
Всего	915	32619

Уязвимости [915]

Идентификатор уязвимости	Уровень опасности	Название уязвимости
BDU:2016-02249	Критический	Adobe Reader и Acrobat до 11.0.18, Acrobat и Acrobat Reader DC Classic до 15.006.30243, и Acrobat и Acrobat Reader DC Continuous до 15.030.20039 позволяет удаленным злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределенных векторов атаки. Уязвимость отлична от CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, и CVE-2016-7019.
сре://a.adobe.acrobat:11	Критический	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-1033-4FFF-7760-000000000000}\DisplayVersion:11.0.03
BDU:2016-00100	Критический	Adobe Reader и Acrobat до 11.0.14, Acrobat и Acrobat Reader DC Classic до 15.006.30119, и Acrobat и Acrobat Reader DC Continuous до 15.010.20056 позволяет удаленным злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределенного вектора атаки.

Для анализа возьмем первую критическую уязвимость из полученного отчета: **BDU:2016-02249**

1. Что уязвимо?

Уязвимы Adobe Acrobat и Adobe Reader на Windows и macOS в версиях до релизов, указанных в бюллетене APSB16-33 (уязвимость входит в набор исправлений, выпущенных в октябре 2016).

Конкретно уязвимые версии — это продукты до версий типа 11.0.18 для Acrobat/Reader 11.x и соответствующих сборок DC/Classic (см. бюллетень для точных номеров сборок).

Классификация уязвимости по типу: нарушение границ буфера / memory corruption (CWE-119), что может привести к удалённому выполнению кода.

2. Как может быть реализована уязвимость? (вектор атаки / эксплуатация)

Вектор: злоумышленник создаёт специально-подготовленный PDF документ, который при открытии в уязвимой версии Acrobat/Reader вызывает ошибку управления памятью (memory corruption).

Результат: возможно удалённое выполнение произвольного кода с привилегиями процесса Acrobat/Reader или отказ в обслуживании (DoS) — в зависимости от детали памяти, которую повреждают. Типичные техники эксплуатации: внедрённый JavaScript в PDF, специально сформированные структуры объектов PDF (stream, font, image, annotation и т. п.) либо некорректная обработка встроенных форматов/сериализованных данных.

Требования для эксплуатации: обычно — пользователь должен открыть/просмотреть вредоносный PDF (social engineering, вложение в e-mail или веб-ссылка). В ряде сценариев может потребоваться определённая комбинация флагов/опций продукта, но общий сценарий — удалённое исполнение при открытии.

Описание на CVE

CVE-2016-7014. Запись в NVD помечена как «Deferred» на странице NVD (не вся дополнительная обработка NVD присутствует), но NVD указывает соответствие с бюллетенем Adobe. Для практических деталей нужно смотреть Adobe APSB16-33 (официальный бюллетень Adobe), где CVE-ID перечислен среди исправленных уязвимостей в октябре 2016.

Описание CVE-2016-7014:

Adobe Reader и Acrobat до версии 11.0.18, Acrobat и Acrobat Reader DC Classic до версии 15.006.30243, а также Acrobat и Acrobat Reader DC Continuous до версии 15.020.20039 в Windows и OS X позволяют злоумышленникам выполнять произвольный код или вызывать отказ в обслуживании (повреждение памяти) через неуказанные векторы, что является уязвимостью, отличной от CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018 и CVE-2016-7019.

Как устраниТЬ уязвимость? (рекомендации)

1. Обновить ПО (главное действие). Установите обновления Adobe Acrobat/Reader, указанные в APSB16-33: обновить до версий, где CVE-2016-7014 исправлена (см. точные номера сборок в бюллетене — например, сборки 11.0.18, 15.006.30243, 15.020.20039 и выше для соответствующих веток). Это единственное корректное исправление уязвимости. helpx.adobe.com

2. Отключить JavaScript в Acrobat/Reader как временную меру снижения риска (если обновление невозможно немедленно) — это уменьшит вектор некоторых PDF-атак (но не гарантирует защиту от всех memory corruption уязвимостей).
3. Включить защищённый режим (Protected Mode / sandbox) и закрыть автоматические функции (например: автоматическое открытие вложений), если продукт это поддерживает.
4. Политики безопасности почты/браузера. Блокировать типы файлов .pdf во входящих письмах от непроверенных отправителей или настроить сканирование вложений антивирусом / sandboxes электронной почты.
5. Мониторинг и IDS/IPS. Внедрить/обновить правила обнаружения в сетевых IPS и почтовых шлюзах для выявления известных сигнатур/связанных эксплойтов (временное смягчение).
6. Минимизация прав. Запускать Acrobat/Reader с минимальными правами, применять политика групп (GPO) для контроля запуска исполняемых файлов и вложений.
7. Регрессионное тестирование. После установки патча — провести проверку (тест открытия ранее проблемных файлов, использование соответствующих тестовых кейсов), убедиться, что сборка обновлена и уязвимость отсутствует.

3. Устранение уязвимости

Для устранения критической уязвимости [BDU:2016-02249](#), которая возникает в старом **Adobe Acrobat Reader v. 11** - данная версия программы была удалена и установлена последняя версия **Adobe Acrobat Reader v. 25**

4. Повторное сканирование хоста

Повторное сканирование хоста после устранения уязвимостей:

The screenshot shows the ScanOVAL application window. At the top, there is a menu bar with 'ScanOVAL' (highlighted in green), 'ГЛАВНОЕ' (Main), and 'СПРАВКА' (Help). Below the menu is a toolbar with icons for download, play, and other functions. A status bar at the top right indicates '2 файла(ов) загружено.' (2 files loaded). The main area contains a table with columns: 'Идентификатор уязвимости' (Vulnerability ID), 'Результат' (Result), 'Уровень о...' (Level), 'Ссылки на источники' (Links to sources), and 'Название уязвимости' (Vulnerability name). A dropdown menu for filtering results is open, showing categories: 'Критический (112)', 'Высокий (142)', 'Средний (190)', and 'Низкий (22)'. At the bottom of the table, there are buttons for 'Группировать по рискам' (Group by risk) and 'Группировать по продуктам' (Group by product), along with numerical counts: 112, 142, 190, and 22. To the right of these buttons is the text 'Всего: 466'. The footer of the window displays the copyright notice '© ФАУ «ГНИИ ПТЗИ ФСТЭК России»'.

Старая версия Adobe Reader содержала очень много критических уязвимостей, поэтому удалив ее и установив последнюю версию было устранено их значительное количество:

Критических - 112 Высоких - 142 Средних - 190 Низких - 22