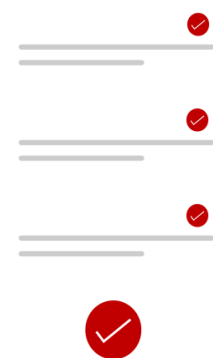


Управление уязвимостями: процессы и инструменты

Александр Дорофеев | Генеральный директор АО «ЭШЕЛОН ТЕХНОЛОГИИ»

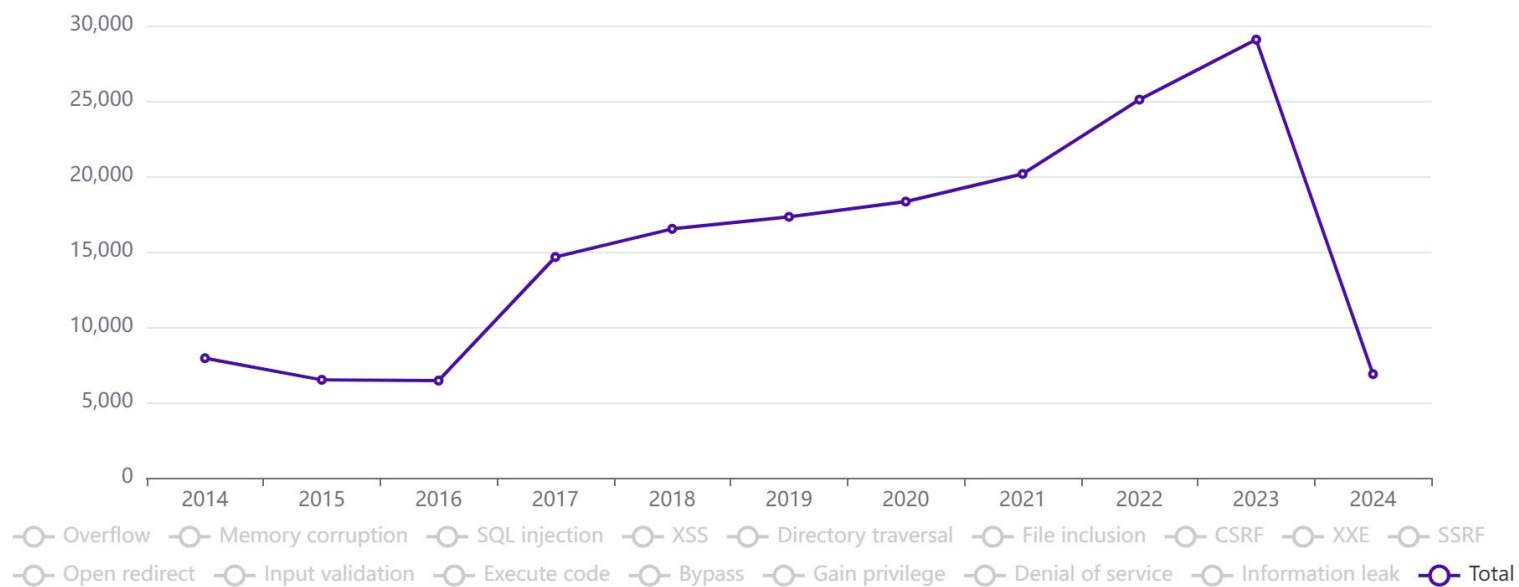
План

1. Актуальность борьбы с уязвимостями
2. Цикл управления уязвимостями
3. Выводы



Количество уязвимостей

Vulnerabilities by type & year



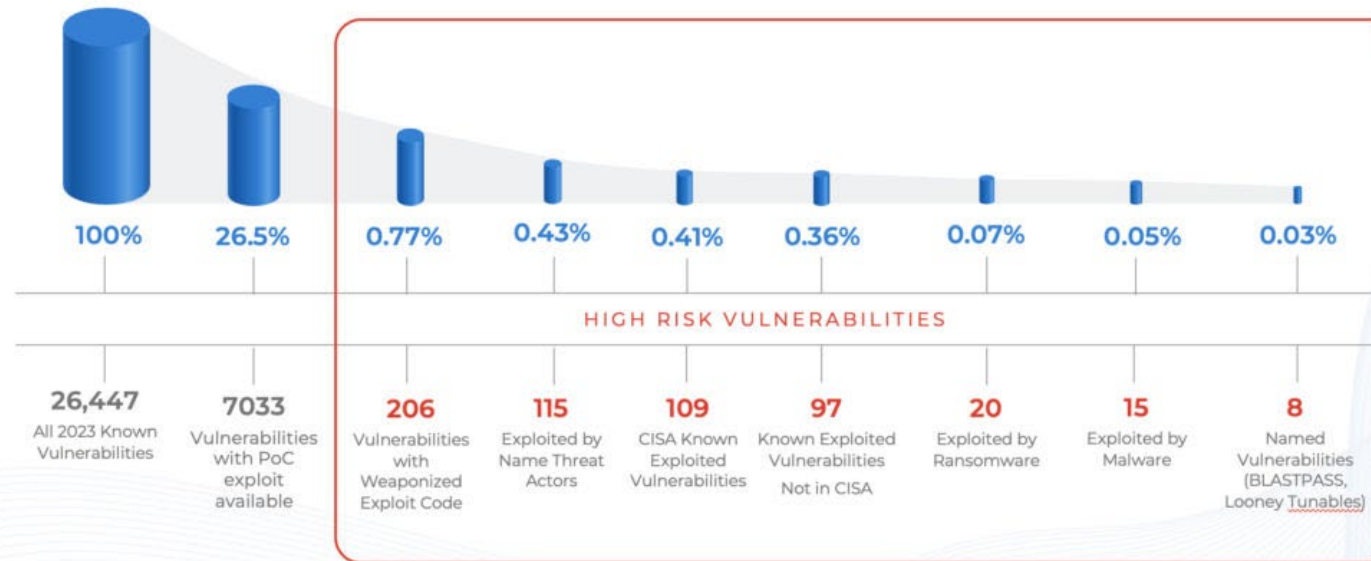
В среднем публикуется более

70

уязвимостей в день

Какой процент реально опасных уязвимостей?

Vulnerability Threat Landscape 2023



Всего уязвимостей

Доказательство возможности эксплуатации

Наличие «боевого» эксплойта

Применение группировками

Наличие в KEV

Эксплуатируемые, но не в KEV

Используемые шифровальщиками

Используемые другими злоредами

Имеющие собственные имена

Источник: <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one>

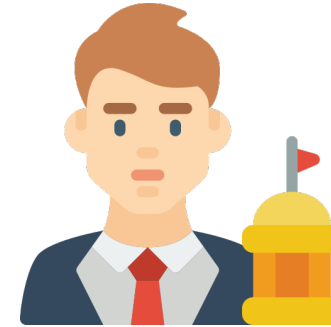
Борьба с уязвимостями



- Разработчик:
 - Процессы разработки безопасного ПО



- Пользователь:
 - Процессы управления уязвимостями



- Регуляторы:
 - Требования к разработчикам СЗИ
 - Методические документы по управлению уязвимостями
 - Ведение базы данных угроз
 - Информирование об уязвимостях

Актуальность

ИСПДН

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+

ГИС

VIII. Контроль (анализ) защищенности информации (АНЗ)				
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+

АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+

КИИ

XIV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+

28. В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрены следующие процессы:

- планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- контроль состояния безопасности значимых объектов критической информационной инфраструктуры;
- совершенствование безопасности значимых объектов критической информационной инфраструктуры.

АСУ ТП

V. Аудит безопасности (АУД)				
АУД.0	Разработка политики аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+

Руководство от ФСТЭК России

МЕТОДИЧЕСКИЙ ДОКУМЕНТ РУКОВОДСТВО ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)

- Для кого:
 - государственных органов
 - организаций, в том числе субъектов КИИ
- Для чего:
 - создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций) и организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
17 мая 2023 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
РУКОВОДСТВО
ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В
ОРГАНЕ (ОРГАНИЗАЦИИ)

2023

Цикл управления уязвимостями



Распределение обязанностей

- Специалисты по информационной безопасности:
 - Мониторинг уязвимостей и оценка их применимости
 - Оценка уязвимостей
 - Определение методов и приоритетов устранения уязвимостей
 - Разработка и реализация компенсирующих мер защиты информации
 - Контроль устранения уязвимостей
 - Разработка предложений по улучшению процесса управления уязвимостями
- Системные администраторы:
 - Устранение уязвимостей
 - Разработка и реализация компенсирующих мер защиты информации

1. МОНИТОРИНГ УЯЗВИМОСТЕЙ И ОЦЕНКА ИХ ПРИМЕНИМОСТИ

- Анализ информации об уязвимости
- Оценка применимости уязвимости
- Принятие решений на получение дополнительной информации
- Постановка задачи на сканирование объектов
- Сканирование объектов
- Оценка защищенности

Источники информации об уязвимостях

- БДУ ФСТЭК России: <https://bdu.fstec.ru/>
- NIST NVD: <https://nvd.nist.gov/>
- Chinese National Vulnerability Database (CNNVD): <https://www.cnvd.org.cn/>
- Debian GNU/Linux Security Bug Tracker
<https://security-tracker.debian.org/tracker/>
- Ubuntu CVE Tracker
<https://people.canonical.com/~ubuntu-security/cve/>
- RHEL/CentOS Security Data
<https://www.redhat.com/security/data/metrics/>

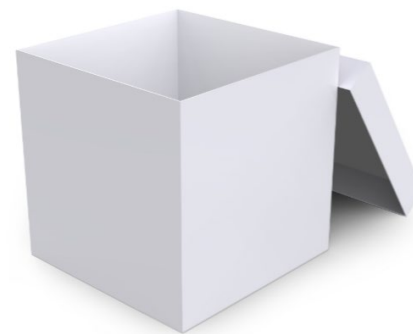
Подходы к тестированию защищенности и «ящики»



Red teaming



Сканирование на наличие уязвимостей



Анализ конфигурации

Комплексный подход: комбинация рассмотренных подходов и приемов злоумышленников

идентификация целевых сетевых узлов

- сбор информации о внешних ресурсах в Интернет
- сканирование сети
- согласование перечня с заказчиком

поиск уязвимостей

- с помощью сканеров
- вручную (по баннерам, ошибки конфигурации)

эксплуатация уязвимостей и проведение атак

- подбор паролей
- перехват трафика
- запуск эксплойтов
- и т.д.

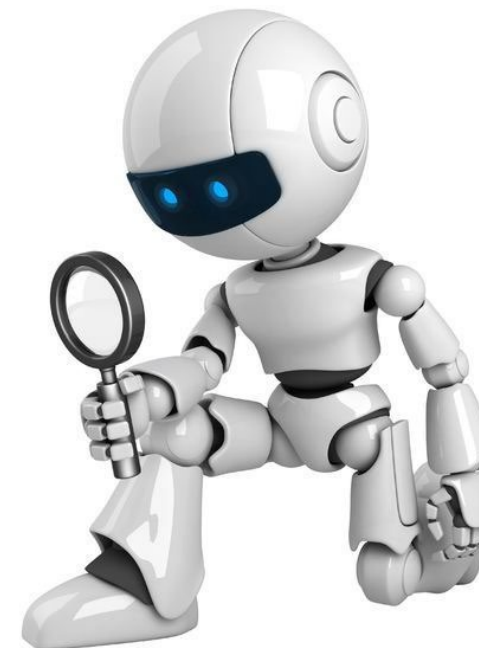
расширение привилегий и зоны влияния

- запуск локальных эксплойтов
- использование собранной информации для доступа к другим системам

Поиск уязвимостей



Ручной



С помощью сканеров

Технология ручного поиска уязвимостей



Apache HTTP Server 2.2.8



apache http server 2.2.8 vulnerabilities

Поиск в Google

Мне повезёт!

Apache » Http Server » 2.2.8 : Security Vulnerabilities (Execute Code)

Cpe-Name: cpe:/a:apache:http_server:2.2.8

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

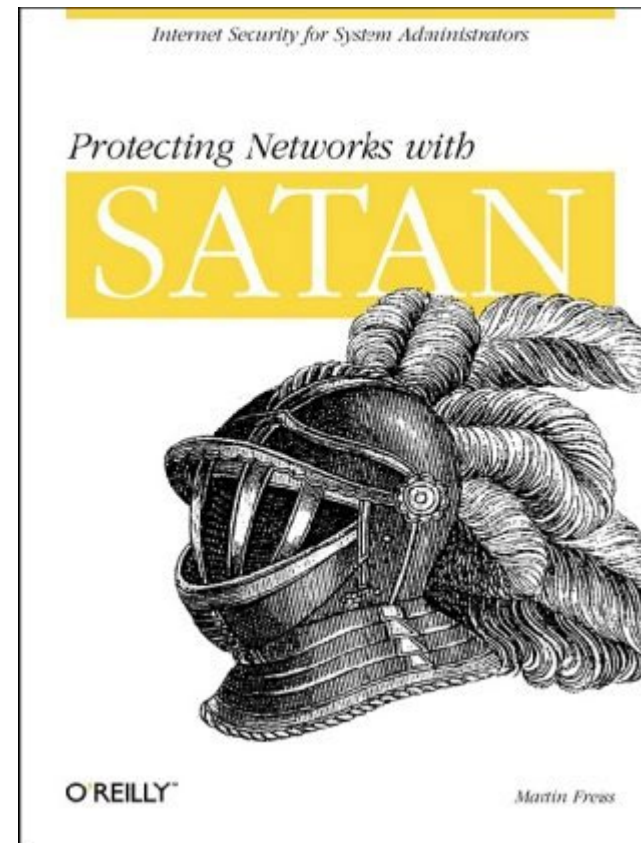
#	CVE ID	CVE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-1862	310		Exec Code	2013-06-10	2017-09-18	5.1	None	Remote	High	Not required	Partial	Partial	Partial
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.														
2	CVE-2010-0425			Exec Code	2010-03-05	2018-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling Isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."														

Total number of vulnerabilities : 2 Page : 1 (This Page)

Первый сканер уязвимостей

- Релиз первого сканера уязвимостей SATAN (Security Administration Tool) состоялся в 5 апреля 1995
- Типы уязвимостей, которые он обнаруживал:
 - Файловые системы NFS, экспортируемые на произвольные хосты
 - Файловые системы NFS, экспортируемые в непривилегированные программы
 - Файловые системы NFS, экспортируемые через portmapper
 - Доступ к файлам с паролями NIS с произвольных хостов
 - Старые (т.е. до версии 8.6.10) версии sendmail
 - Доступ к REXD с произвольных хостов
 - отключен контроль доступа к X-серверу
 - доступ к произвольным файлам через TFTP
 - удаленный доступ к оболочке с произвольных хостов
 - доступный для записи домашний каталог анонимного FTP
- Написан на Perl и shell-скриптах

Сайт: <http://www.porcupine.org/satan/>



Запуск скриптов для проверок до сих пор применяется

Nessus Attack
Scripting Language

Nmap Scripting Engine

```
Открыть  apache_2_2_8_nasl  Сохранить
~/Documents/plugins

script_set_attribute(attribute:"exploit_available", value:"true");
script_cwe_id(79, 399);

script_set_attribute(attribute:"plugin_publication_date", value:"2008/02/20");
script_set_attribute(attribute:"vuln_publication_date", value:"2007/11/14");

script_set_attribute(attribute:"plugin_type", value:"remote");
script_set_attribute(attribute:"cpe", value:"cpe:/a:apache:http_server");
script_end_attributes();

script_category(ACT_GATHER_INFO);
script_family(english:"Web Servers");

script_copyright(english:"This script is Copyright (C) 2008-2018 Tenable Network Security, Inc.");

script_dependencies("apache_http_vernon.nasl");
script_require_keys("installed_sw/Apache");
script_require_ports("Services/www", 80);

exit(0);
}

include("global_settings.inc");
include("misc_func.inc");
include("reporting.inc");
include("audit.inc");
include("install_func.inc");

get_install_count(app_name:"Apache", exit_if_zero:TRUE);
port = get_http_port(default:80);
install = get_single_install(app_name:"Apache", port:port, exit_if_unknown_ver:TRUE);

# Check if we could get a version first, then check if it was
# backported
version = get_kb_item_or_exit('www/apache/'+port+'/version', exit_code:1);
backported = get_kb_item_or_exit('www/apache/'+port+'/backported', exit_code:1);

if (report_paranoia < 2 && backported) audit(AUDIT_BACKPORT_SERVICE, port, "Apache");
source = get_kb_item_or_exit('www/apache/'+port+'/source', exit_code:1);

# Check if the version looks like either ServerTokens Major/Minor
# was used
if (version =~ '^2(\.|\d)?S') exit(1, "The banner from the Apache server listening on port "+port+" - "+source+" - is not granular enough to make a determination.");
if (version =~ '^(\d+(\.\d+)?S)') exit(1, "The version of Apache listening on port " + port + " - "+ source + " - is non-numeric and, therefore, cannot be used to make a determination.");
if (version =~ '^2(\.|\d)?' && ver_compare(ver:version, fix:'2.2.8') == -1)
{
  set_kb_item(name:"www/"+port+"/XSS", value:TRUE);
  if (report_verbosity > 0)
  {
    report =
    '\n Version source      : ' + source +
    '\n Installed version  : ' + version +
    '\n Fixed version      : 2.2.8\n';
    security_warning(port:port, extra:report);
  }
}
```

Текст Ширина таблицы: 8 Стр 115, Стлб 4 ВСТ

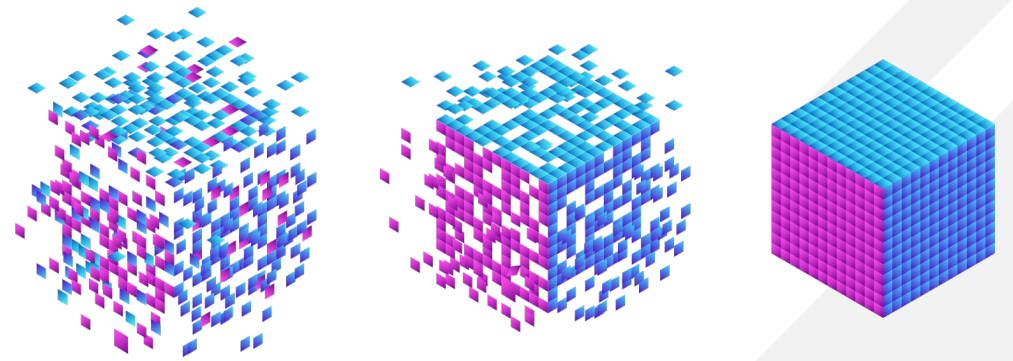
Проблемы скриптового подхода

- Нужно поддерживать несколько десятков тысяч плагинов/скриптов, выявляющих уязвимости.
- Сканирование одного узла может занимать десятки минут.



Современный подход: использование агрегированной базы данных уязвимостей

- БДУ ФСТЭК России
- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- ...



Сканер-ВС 6: основные функции

The screenshot displays the main dashboard of the Scaner-BS 6 application. At the top, there is a navigation bar with a star icon and the word 'ЗАДАЧИ' (Tasks). Below it, a secondary menu contains 'Активы' (Assets), 'Задачи' (Tasks), 'Отчеты' (Reports), 'Карты сети' (Network Maps), 'Инструменты' (Tools), and 'Администрирование' (Administration). On the right side of the navigation bar, the current project is identified as 'Проект_01', and the user is logged in as 'admin'.

Below the navigation bar, there is a breadcrumb trail: 'Главная / Список задач / Новая задача' (Home / Task List / New Task). The main heading for this section is 'Новая задача' (New Task).

The dashboard features five prominent function cards, each with an icon and a brief description:

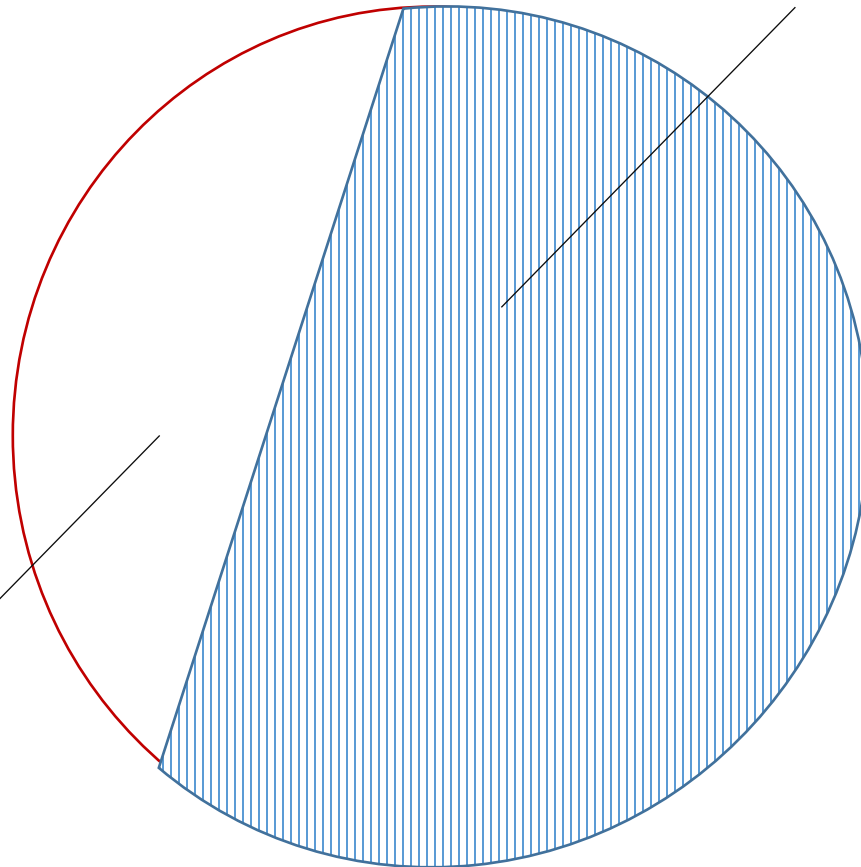
- Исследование сети** (Network Research): Scанирование сетевых узлов и сервисов, идентификация ОС и приложений, трассировка сетевых маршрутов для построения топологии сети.
- Инвентаризация** (Inventory): Использование активного подключения к исследуемому узлу для сбора информации.
- Поиск уязвимостей** (Vulnerability Search): Выявление уязвимостей программного обеспечения.
- Подбор паролей** (Password Selection): Проверка стойкости паролей сетевых сервисов.
- Аудит** (Audit): Проверка настроек программного обеспечения на соответствие требованиям безопасности.

Источник информации о версиях: сетевое сканирование и инвентаризация

Все программные пакеты, включая локальные.
Требуется административный доступ по SSH/WinRM.



Сетевые сервисы:
требуется только доступ по сети



2. ОЦЕНКА УЯЗВИМОСТЕЙ

- Получение информации об объектах, подверженных уязвимости
- Определение уровня опасности уязвимости
- Определение влияния на информационные системы
- Расчет критичности уязвимости

От чего зависит наше восприятие опасности уязвимости?

- Внешние факторы:
 - Оценка уязвимости по CVSS
 - Оценка потенциальной возможности эксплуатации (EPSS)
 - Наличие опубликованных эксплойтов
- Внутренние факторы:
 - Доступность актива извне
 - Особенности ИТ-инфраструктуры
 - Особенности конфигурации систем
 - Критичность активов с точки зрения бизнеса

Степень опасности уязвимости

- Common Vulnerability Scoring System (CVSS) — это открытый стандарт, используемый для расчета количественной оценки степени опасности.
- При расчете учитываются такие факторы, как наличие эксплойта, возможность удаленной эксплуатации, необходимость авторизации, возможные последствия.
- Калькуляторы для расчета CVSS 2/3/3.1:
<https://bdu.fstec.ru/calc>

Оценка по CVSS v4: CVE-2022-41741

CVSS v4 Score: Base 7.3

Metric	Value	Comments
Attack Vector	Local	У атакующего должен быть интерактивный доступ к системе
Attack Complexity	Low	Специальных условий и знаний не требуется
Attack Requirements	Present	Для успешной эксплуатации этой уязвимости необходимо выполнить множество условий, требующих сбора информации и подготовки цели.
Privileges Required	Low	Атакующий должен иметь возможность поместить файл в корневой каталог NGINX.
User Interaction	None	Взаимодействия с пользователем не требуется
Vulnerable System Confidentiality	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Vulnerable System Integrity	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Vulnerable System Availability	High	Злоумышленник может выполнить произвольный код на уязвимой системе с повышенными привилегиями.
Subsequent System Confidentiality	None	Это не повлияет на последующую конфиденциальность системы.
Subsequent System Integrity	None	Это не повлияет на последующую целостность системы.
Subsequent System Availability	None	Это не повлияет на последующую доступность системы.

Определение степени опасности уязвимости

- CVSSv2:
 - Низкая (Low) – 0.0 – 3.9
 - Средняя (Medium) – 4.0 – 6.9
 - Высокая (High) – 7.0 – 10.0
- CVSSv3/v3.1/v4:
 - Не определен (None) – 0.0
 - Низкая (Low) – 0.1 – 3.9
 - Средняя (Medium) – 4.0 – 6.9
 - Высокая (High) 7.0 – 8.9
 - Критическая (Critical) – 9.0 – 10.0



CVE

- CVE (Common Vulnerabilities and Exposures) — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

- <https://www.cve.org/>

← → ↻ 🔒 cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

CVE-ID	
CVE-2011-2523	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• MISC:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html• MISC:https://access.redhat.com/security/cve/cve-2011-2523• MISC:https://packetstormsecurity.com/files/102745/Vsftpd-2.3.4-Backdoor-Command-Execution.html• MISC:https://security-tracker.debian.org/tracker/CVE-2011-2523• MISC:https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805• MLIST:[oss-security] 20110711 Re: vsftpd download backdoored• URL:https://www.openwall.com/lists/oss-security/2011/07/11/5	
Assigning CNA	
Red Hat, Inc.	
Date Record Created	
20110615	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily reflect when the record was updated in CVE.
Phase (Legacy)	
Assigned (20110615)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is a record on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

Идентификаторы CVE и BDU в Сканер-ВС 6

ЗАДАЧИ Активы **Задачи** Отчеты Карты сети Инструменты Администрирование

Проект_01 Ru admin

Главная / Список задач / Поиск уязвимостей / Уязвимое ПО / Internet explorer

Уязвимое ПО История

Поиск

☐	CVE	BDU	CVSS2 балл	CVSS3 балл	Уровень критичности
<input type="checkbox"/>	CVE-2016-3325	BDU:2016-02156	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2016-3321	BDU:2016-01960	1,9	2,5	Низкий
<input type="checkbox"/>	CVE-2016-7199	BDU:2016-02406	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2016-7227	BDU:2016-02363	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2016-3274	BDU:2016-01880	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2016-3276	BDU:2016-01879	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2016-3291	BDU:2016-02165	2,6	2,4	Низкий
<input type="checkbox"/>	CVE-2016-3351	BDU:2016-02148	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2018-0942	–	2,1	2,6	Низкий
<input type="checkbox"/>	CVE-2016-7239	BDU:2016-02360	2,6	3,1	Низкий
<input type="checkbox"/>	CVE-2015-0055	–	4,3	–	Средний
<input type="checkbox"/>	CVE-2014-6365	–	4,3	–	Средний
<input type="checkbox"/>	CVE-2014-0268	BDU:2014-00206	4,3	–	Средний
<input type="checkbox"/>	CVE-2015-0054	–	4,3	–	Средний
<input type="checkbox"/>	CVE-2014-6350	–	4,3	–	Средний

Отображать на странице: 25 1-25 из 718 элементов 1 из 29 страниц

Карточка уязвимости в Сканер-ВС 6

The screenshot displays the Scaner-BS 6 web interface. The top navigation bar includes 'ЗАДАЧИ', 'Активы', 'Задачи', 'Отчеты', 'Карты сети', 'Инструменты', and 'Администрирование'. The user is logged in as 'admin' in the 'Проект_01' environment. The main content area shows a vulnerability card for CVE-2019-12761, categorized as 'Высокий' (High). The card includes a description of the issue in PyXDG, a table of identifiers (CVE, BDU, CVSS2 vector, CVSS2 балл, CVSS3 vector, CVSS3 балл), and a table of product information (Name: python3-xdg, Version: 0.25-5). On the right, a configuration snippet for 'debian' is shown, detailing the 'fixed' version '0.26-1'.

Главная / Список задач / Поиск уязвимостей / Уязвимое ПО / python3-xdg /
Информация по найденной уязвимости

Высокий

CVE-2019-12761

Информация об уязвимости

Описание

Проблема с внедрением кода была обнаружена в PyXDG до 0.26 с помощью созданного кода Python в элементе Категории XML-документа меню в файле .menu. XDG_CONFIG_DIRS должен быть настроен для запуска синтаксического анализа xdg.Menu.parse в каталоге, содержащем этот файл. Это связано с отсутствием дезинфекции в xdg/Menu.py перед вызовом на оценку.

CVE	CVE-2019-12761
БДУ	BDU:2021-05299
CVSS2 вектор	AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS2 балл	5.1
CVSS3 вектор	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
CVSS3 балл	7.5

Информация по уязвимому ПО

Название	python3-xdg
Связанные названия	python3-xdg, pyxdg
Версия	0.25-5

Рекомендации **Конфигурация** Эксплойты

```
debian
1 {
2   "os_name": "debian",
3   "soft_name": "pyxdg",
4   "trait": {
5     "fixed": "0.26-1"
6   }
7 }
```

EPSS

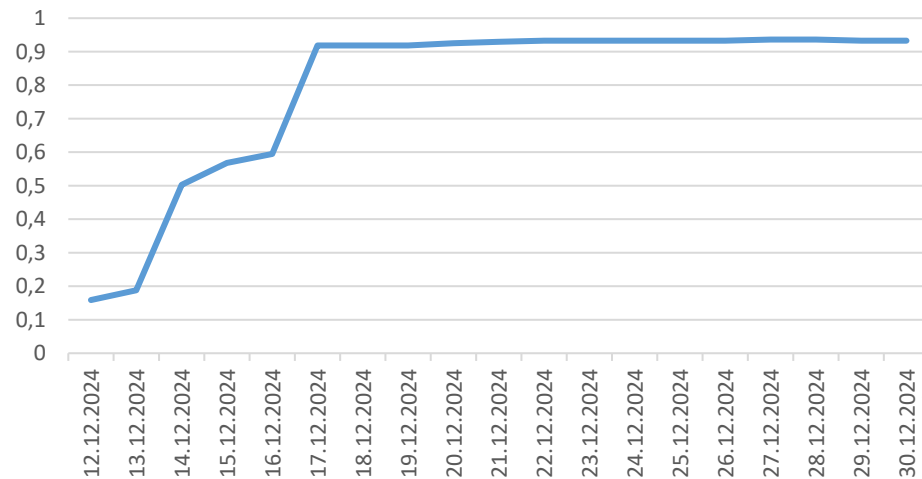
- EPSS предоставляет возможности для эффективного управления уязвимостями на основе данных. Основана на данных и использует текущую информацию об угрозах из CVE и реальные данные об эксплойтах.
- Модель EPSS выдает оценку вероятности от 0 до 1 (от 0 до 100 %), где чем выше оценка, тем больше вероятность того, что уязвимость будет использована.

Как работает модель EPSS?

1. Сбор информации об уязвимостях из различных источников.
2. Сбор информации об ежедневной активности по эксплуатации.
3. Обучение модели: выявление взаимосвязей между информацией об уязвимостях и активностью по эксплуатации.
4. Измерение производительности модели и повторение 3 шага для оптимизации модели.
5. Ежедневное обновление информации об уязвимостях (шаг 1) и использование модели (шаг 3) для получения ежедневных оценок вероятности эксплуатации в течение следующих 30 дней для каждого опубликованного CVE.

Уязвимость Log4shell

EPSS CVE-2021-44228



24.11.21

26.11.21

06.12.21

09.12.21

10.12.21

12.12.21

17.12.21

Chen Zhaojun
Обнаруживает
уязвимость

Резервирование
идентификатора
CVE-2021-44228

Выпуск Log4j
2.15.0,
в которой
закрота
уязвимость

Публикация
в Твиттере

Публикация
информации об
уязвимости
CVE-2021-44228

Появилась
оценка EPSS

Повышение уровня опасности
до критического, так как 2.15.0
все уязвимы.

Где публикуются эксплойты?

The screenshot shows the Exploit-DB website interface. At the top, there's a navigation bar with the site logo and search filters. Below that, a table lists various exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. The table shows 15 entries, with the first one being 'vm2 - sandbox escape' by Calli Khalil. Below the table, there's a pagination bar showing 'Showing 1 to 15 of 45,928 entries' and navigation links like 'FIRST', 'PREVIOUS', '1', '2', '3', '4', '5', '3062', 'NEXT', and 'LAST'. At the bottom, there's a dark blue navigation menu with four categories: Databases, Links, Sites, and Solutions, each with a list of sub-links.

Date	D	A	V	Title	Type	Platform	Author
2024-03-16	↓		×	vm2 - sandbox escape	Local	Multiple	Calli Khalil
2024-03-16	↓		×	UPS Network Management Card 4 - Path Traversal	WebApps	PHP	Victor Garcia
2024-03-16	↓		×	Nokia BMC Log Scanner - Remote Code Execution	WebApps	Linux	Carlos Andres Gonzalez, Matthew Gregory
2024-03-16	↓		×	Karaf v4.4.3 Console - RCE	WebApps	Java	Andrzej Olchawa, Milenko Starcik
2024-03-16	↓		×	LaborOfficeFree 19.10 - MySQL Root Password Calculator	Local	Windows	Peter Gabaldon
2024-03-16	↓		×	Winter CMS 1.2.3 - Server-Side Template Injection (SSTI) (Authenticated)	WebApps	PHP	tmrswrr
2024-03-14	↓		×	KITTY 0.76.1.13 - Command Injection	Local	Windows	DEFCESCO
2024-03-14	↓		×	KITTY 0.76.1.13 - 'Start Duplicated Session Username' Buffer Overflow	Local	Windows	DEFCESCO
2024-03-14	↓		×	KITTY 0.76.1.13 - 'Start Duplicated Session Hostname' Buffer Overflow	Local	Windows	DEFCESCO
2024-03-14	↓		×	GitLab CE/EE < 16.7.2 - Password Reset	Remote	Java	0xB455
2024-03-14	↓		×	Ruijie Switch PSG-5124 26293 - Remote Code Execution (RCE)	Remote	Hardware	ByteHunter
2024-03-14	↓		×	Viessmann Vitogate 300 2.1.3.0 - Remote Code Execution (RCE)	Remote	Hardware	ByteHunter
2024-03-14	↓		×	SolarView Compact 6.00 - Command Injection	Remote	Hardware	ByteHunter
2024-03-14	↓		×	Honeywell PM43 < P10.19.050004 - Remote Code Execution (RCE)	Remote	Hardware	ByteHunter
2024-03-14	↓		×	JetBrains TeamCity 2023.05.3 - Remote Code Execution (RCE)	Remote	Java	ByteHunter

Showing 1 to 15 of 45,928 entries

FIRST PREVIOUS 1 2 3 4 5 ... 3062 NEXT LAST

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

Информация о доступных эксплойтах

The screenshot displays a web application interface with a navigation menu at the top: ЗАДАЧИ, Активы, Задачи (highlighted), Отчеты, Карты сети, Инструменты, and Администрирование. The user is logged in as 'admin' in the 'Проект_01' environment. The main content area is divided into two panels. The left panel shows the details for CVE-2009-3272, including a description of a stack overflow vulnerability in WebKit.dll and a table of associated metrics. The right panel shows search results for 'exploitdb' with a link to a specific exploit on exploit-db.com.

Главная / Список задач / Поиск уязвимостей / Уязвимое ПО / libqt4-opengl /
Информация по найденной уязвимости

Средний

CVE-2009-3272

Информация об уязвимости

Описание

Уязвимость потребления стека в WebKit.dll в WebKit в Apple Safari 3.2.3 и, возможно, в других версиях до 4.1.2, позволяет удаленным злоумышленникам вызывать отказ в обслуживании (сбой приложения) с помощью кода JavaScript, который вызывает eval в длинной строке, состоящей из последовательностей/.

CVE	CVE-2009-3272
БДУ	—
CVSS2 вектор	AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS2 балл	5
CVSS3 вектор	—
CVSS3 балл	—

Информация по уязвимому ПО

Название	libqt4-opengl
Связанные названия	libqt4-opengl, qt4-x11
Версия	4:4.8.7+dfsg-20astra3

Рекомендации | Конфигурация | **Эксплоиты**

exploitdb
<https://www.exploit-db.com/exploits/9606>

Теги и критичность

The screenshot shows a web application interface for managing active devices. The top navigation bar includes a star icon, the word 'АКТИВЫ', and several menu items: 'Активы', 'Задачи', 'Отчеты', 'Карты сети', 'Инструменты', and 'Администрирование'. On the right, there are options for 'Проект_01', 'Ru', and 'admin'. Below the navigation bar, there is a breadcrumb 'Главная / Активы', a search bar with the text 'Поиск', and a button 'Добавить актив +'. The main content area features a table with the following columns: 'Название', 'IPv4', 'Тип устройства', 'Тип ОС', 'Теги', 'Создано', and 'Обновлено'. The table contains five rows of data, each with a checkbox, a criticality icon, and a tag. The footer of the interface shows 'Отображать на странице: 25' and '1-5 из 5 элементов', along with pagination controls for '1 из 1 страниц'.

	⚠	Название	IPv4	Тип устройства	Тип ОС	Теги	Создано	Обновлено
<input type="checkbox"/>	⚠	Windows10	10.0.5.171	рабочая станция	Windows	Производство	19.03.2024, 09:45:11	19.03.2024, 10:18:39
<input type="checkbox"/>	⚠	Ubuntu 20.04	10.0.5.84	виртуальная машина	Linux	Разработка	19.03.2024, 09:46:44	19.03.2024, 10:53:26
<input type="checkbox"/>	⚠	Astra Linux 1.7.4	10.0.5.50	сервер	Linux	Бухгалтерия	19.03.2024, 09:46:13	19.03.2024, 10:19:25
<input type="checkbox"/>	✅	Debian 11	10.0.5.138	другое	Linux	Маркетинг	19.03.2024, 09:47:48	19.03.2024, 10:55:07
<input type="checkbox"/>	⚠	Windows server 2016	10.0.5.65	сервер	Windows	Продажи	19.03.2024, 09:57:33	19.03.2024, 10:53:58

3. ОПРЕДЕЛЕНИЕ МЕТОДОВ И ПРИОРИТЕТОВ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

- Определение приоритетности устранения уязвимостей
- Определение методов устранения уязвимостей
- Принятие решения о срочной установке обновлений
- Создание заявки на срочную установку обновления
- Принятие решения о срочной реализации компенсирующих мер защиты информации
- Создание заявки на установку обновления
- Создание заявки на реализацию компенсирующих мер защиты информации

4. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

- Согласование установки с руководством подразделения ИТ
- Тестирование обновления
- Установка обновления в тестовом сегменте
- Принятие решения об установке обновления
- Установка обновления
- Формирование плана установки обновлений
- Разработка и реализация компенсирующих мер защиты информации

Способы устранения уязвимостей

- Установка патча или новой версии
- Отключение сетевой службы, если есть возможность ее заменить или отказаться вовсе
- Ограничение доступа к уязвимому сервису или активу (например, ограничение по IP)
- Использование средств защиты, блокирующих эксплуатацию уязвимости (IPS, WAF, AV)



Рекомендуемые сроки устранения уязвимостей

- критический уровень опасности до 24 часов
- высокий уровень опасности – до 7 дней
- средний уровень опасности – до 4 недель
- низкий уровень опасности – до 4 месяцев

5. Контроль устранения уязвимостей

- Принятие решения о способе контроля
- Проверка объектов на наличие уязвимостей
- Оценка защищенности
- Выявление отклонений и неисполнений
- Разработка предложений по улучшению процесса управления уязвимостями



Запуск по расписанию и отправка событий в SIEM

★ ЗАДАЧИ Активы Задачи Отчеты Карты сети Инструменты Администрирование Проект_01 Ru admin

Главная / Список задач / Новая задача / Инвентаризация

Инвентаризация

Настройки **Расписание**

Запуск задачи по расписанию

1 раз По расписанию

Расписание запросов (Cron)

20 2 * 1,2,3 * Заполнить вручную

Минуты Часы Дни Месяцы Дни недели

Конкретное значение

20

Сохранить

Выводы

- Процессы управления уязвимостями достаточно хорошо проработаны методически.
- Инструментарий для ключевого процесса по выявлению уязвимостей разработан и доступен.
- Ключевым навыком экспертов является приоритезация уязвимостей.

Спасибо!

Сканер-ВС 6 в телеграм

