ТРЕНДОВЫЕ УЯЗВИМОСТИ 2025

АЛЕКСАНДР ЛЕОНОВ
Ведущий эксперт PT Expert Security Center
Positive Technologies

О себе

- Леонов Александр
- Занимаюсь в Vulnerability Management-ом с 2009
- Работаю в PT Expert Security Center
- Веду Telegram-канал

"Управление Уязвимостями и прочее"

t.me/avleonovrus

CVE.ICU

Home | Yearly Analysis | CNA | CPE | CWE | Scoring | Growth | Calendar

42 792
CVEs This Year

127.4
Avg CVEs/Day

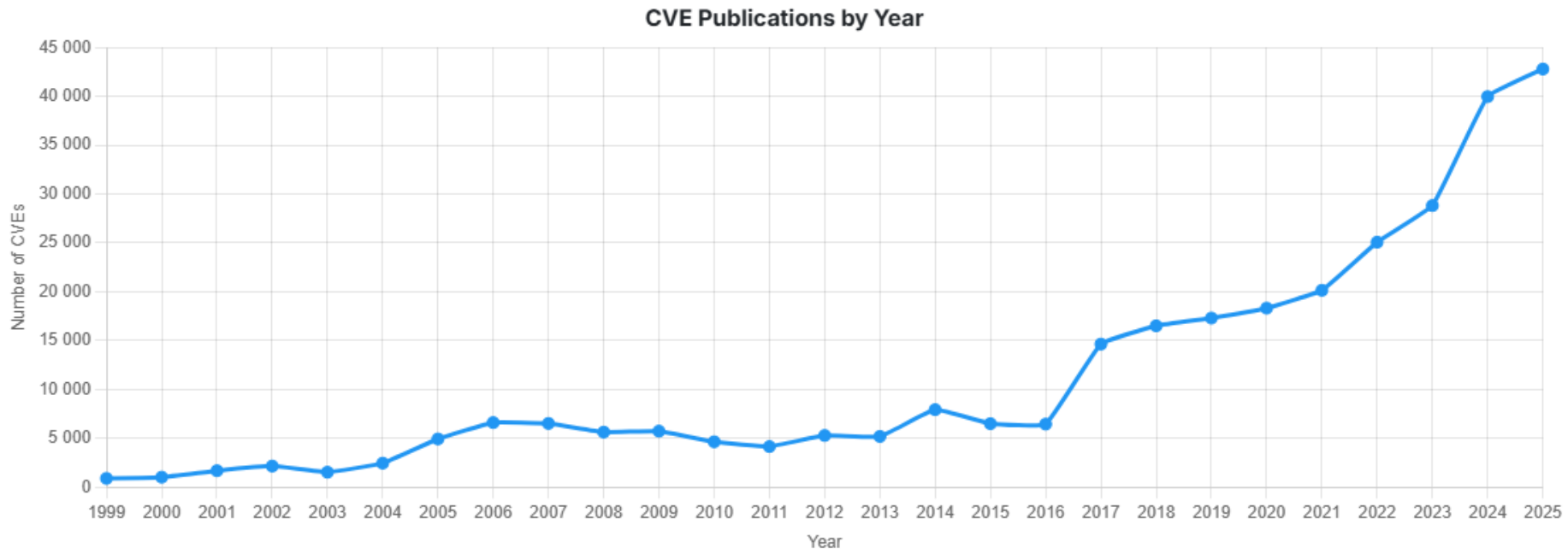
+18%
YOY Growth
42 792 vs 36 251 (YTD vs Same Period 2024)

302 859
Total CVEs

1 463
Known Exploited CVEs
CISA KEV catalog across all years

CVE Publications by Year

Historical trend of vulnerability disclosures from 1999 to present



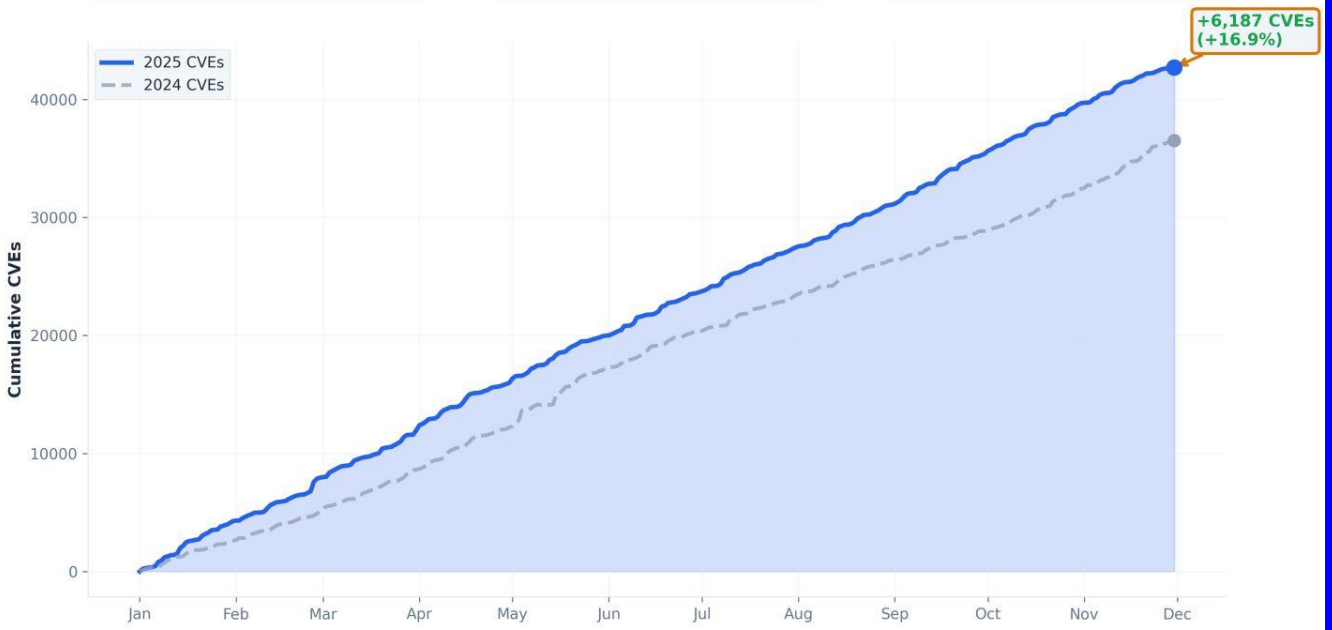
View Full Dashboard →

Jerry Gamblin

2025 CVE Growth Report

Data through November 30, 2025

Total CVEs	YoY Growth	Daily Average
42,697	+16.9%	128
Through November	vs 2024 (36,510)	CVEs per day



Peak: Sep (4,322) | Low: Nov (3,028) | Highest YoY: Sep (+71.8%)

Data: NIST National Vulnerability Database | @jgamblin | rogolabs.net

https://nvd.nist.gov/general/nvd-dashboard

2024

CVE Status Count

Total	272243
Received	223
Awaiting Analysis	20619
Undergoing Analysis	741
Modified	229241
Rejected	14491

NVD Contains

CVE Vulnerabilities	272243
Checklists	807
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	0
CPE Names	1338946

https://nvd.nist.gov/general/nvd-dashboard

2024

CVE Status Count

Total	272243
Received	223
Awaiting Analysis	20619
Undergoing Analysis	741
Modified	229241
Rejected	14491

NVD Contains

CVE Vulnerabilities	272243
Checklists	807
US-CERT Alerts	249

2025

CVE Status Count

Total	319756
Received	62
Awaiting Analysis	26202
Undergoing Analysis	730
Modified	138952
Deferred	94583
Rejected	16193

NVD Contains

CVE Vulnerabilities	319745
Checklists	847
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	0
CPE Names	1516300

Трендовые уязвимости

Уязвимости, которые активно используются в атаках или с высокой степенью вероятности будут использоваться в ближайшее время.

+ актуальны для России

NVD

~ 40 000

2024

Трендовые

74

NVD

> 42 000

2025

(предварительно)

Трендовые

63

Киберугрозы/инциденты

Ноябрьский дайджест трендовых уязвимостей

13 НОЯБРЯ 2025

ПОДЕЛИТЬСЯ

Содержание:

По итогам анализа, проведенного экспертами Positive Technologies, мы публикуем список уязвимостей, которые отнесли к списку трендовых. Это самые опасные недостатки безопасности, которые уже активно эксплуатируются злоумышленниками или могут быть использованы ими в

@ptsecurity 13 ноя в 14:51

Ноябрьский «В тренде VM»: уязвимости в продуктах Microsoft, Redis, XWiki, Zimbra Collaboration и Linux

11 мин 6.8K

Блог компании Positive Technologies, Информационная безопасность*, Тестирование IT-систем*, SharePoint*, Linux*

Дайджест

Хабр, привет! На связи Александр Леонов, ведущий эксперт PT Expert Security Center и дежурный по самым опасным уязвимостям месяца. Мы с командой аналитиков Positive Technologies регулярно исследуем информацию об уязвимостях из баз и бюллетеней безопасности вендоров, социальных сетей, блогов, телеграм-каналов, баз эксплойтов, публичных репозиториев кода и выявляем во всем этом многообразии сведений трендовые уязвимости. Это те уязвимости, которые либо уже эксплуатируются вживую, либо будут эксплуатироваться в ближайшее время.

Идентификатор уязвимости

Выберите идентификатор

Рейтинг уязвимости

- [ ] Критический
- [ ] Высокий
- [ ] Средний
- [ ] Низкий
- [ ] Без рейтинга

Стала трендовой

Год

Месяц

Вендор

Вендор

КРИТИЧЕСКИЙ – 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVE-2025-64459

Уязвимость в Django, связанная с некорректной обработкой словарей в запросах GET и POST. Эксплуатация уязвимости позволяет злоумышленнику, не прошедшему аутентификацию, выполнить произвольный SQL-запрос. Для уязвимости существует общедоступный эксплойт.

Вендор:	Django
Уязвимый продукт:	Django
CVE ID:	CVE-2025-64459
Стала трендовой:	18 ноября 2025

ВЫСОКИЙ – 7 AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2025-62215

Уязвимость в ядре Windows, связанная с состоянием гонки. Эксплуатация уязвимости позволяет злоумышленнику повысить уровень своих привилегий до системных (SYSTEM). Для эксплуатации уязвимости атакующему необходимо выиграть в состоянии гонки. Зафиксированы случаи использования уязвимости в реальных атаках.

Вендор:	Microsoft
Уязвимый продукт:	Windows, Windows Server
CVE ID:	CVE-2025-62215
Стала трендовой:	12 ноября 2025

БЕЗ РЕЙТИНГА

CVE-2025-12735

Уязвимость в библиотеках expr-eval и expr-eval-fork для Node.js. Уязвимость связана с недостаточной проверкой входных данных и позволяет злоумышленнику, действующему удаленно, выполнить произвольный JavaScript-код в контексте приложения.

Вендор:	
Уязвимый продукт:	
CVE ID:	
Стала трендовой:	

https://avleonov.com/vulristics_reports/pt_trend_cve_combined2025_report_with_comments_ext_img.html

Vulristics

Report Name: pt_trend_cve_combined2025
Generated: 2025-11-27 23:22:15

Vulristics Vulnerability Scores

- All vulnerabilities: 63
- Urgent: 39
- Critical: 17
- High: 4
- Medium: 3
- Low: 0

Basic Vulnerability Scores

- All vulnerabilities: 63
- Critical: 23
- High: 30
- Medium: 7
- Low: 0

Products

Product Name	Prevalence	U	C	H	M	L	A	Comment
Apache HTTP Server	0.9	1					1	Apache HTTP Server is a free and open-source web server that delivers web content through the internet
Django	0.9		1				1	Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. It provides built-in tools for database models, authentication, URL routing, templates, and security features, making it one of the most widely used frameworks for building scalable and maintainable web applications.
Linux Kernel	0.9			1			1	The Linux kernel is a free and open-source, monolithic, modular, multitasking, Unix-like operating system kernel
Sudo	0.9	1					1	Sudo is a widely used Unix/Linux utility that allows permitted users to execute commands with elevated (typically root) privileges while providing extensive logging and fine-grained security controls. It is a foundational component in most Linux and BSD distributions.
Windows Kernel	0.9	1					1	Windows Kernel

Vulnerability Types

Vulnerability Type	Criticality	U	C	H	M	L	A
Remote Code Execution	1.0	19	7	2	2		30
Authentication Bypass	0.98	3			1		4
Code Injection	0.97		1				1
Security Feature Bypass	0.9	1					1
Elevation of Privilege	0.85	12	6	1			19
Arbitrary File Reading	0.83			1			1
Information Disclosure	0.83		1				1
Cross Site Scripting	0.8	2	1				3
Memory Corruption	0.5		1				1
Spoofing	0.4	2					2

Exploitation in the wild detected (47)

Remote Code Execution (21)

- Apache HTTP Server (CVE-2024-38475)
- Windows Server Update Service (WSUS) (CVE-2025-59287)
- Apache Tomcat (CVE-2025-24813)
- XWiki Platform (CVE-2025-24893)
- WinRAR (CVE-2025-6218, CVE-2025-8088)
- Microsoft SharePoint (CVE-2025-49704)
- Roundcube (CVE-2025-49113)
- Control Web Panel (CVE-2025-48703)
- Windows Fast FAT File System Driver (CVE-2025-24985)
- Microsoft SharePoint Server (CVE-2025-53770)
- SAP NetWeaver (CVE-2025-31324, CVE-2025-42999)
- Internet Shortcut Files (CVE-2025-33053)
- Erlang/OTP (CVE-2025-32433)
- 7-Zip (CVE-2025-0411)
- Cisco ASA (CVE-2025-20333)
- ESXi (CVE-2025-22224)
- Windows NTFS (CVE-2025-24993)
- Windows LNK File (CVE-2025-9491)
- CommuniGate Pro (BDU:2025-01331)

Elevation of Privilege (15)

- Windows SMB Client (CVE-2025-33073)
- Sudo (CVE-2025-32463)
- Windows Hyper-V NT Kernel Integration VSP (CVE-2025-21333, CVE-2025-21334, CVE-2025-21335)
- Windows Agere Modem Driver (CVE-2025-24990)
- Microsoft DWM Core Library (CVE-2025-30400)
- Windows Common Log File System Driver (CVE-2025-29824, CVE-2025-32701, CVE-2025-32706)
- Windows Kernel (CVE-2025-62215)
- Windows Win32 Kernel Subsystem (CVE-2025-24983)
- Windows Ancillary Function Driver for WinSock (CVE-2025-21418)

Public exploit exists, but exploitation in the wild is NOT detected (12)

Remote Code Execution (7)

- Windows Lightweight Directory Access Protocol (LDAP) (CVE-2024-49112)
- Windows OLE (CVE-2025-21298)
- Kubernetes (CVE-2025-1974)
- Redis (CVE-2025-49844)
- Microsoft Configuration Manager (CVE-2024-43468)
- 7-Zip (BDU:2025-01793, CVE-2025-55188)

Elevation of Privilege (4)

- Windows Cloud Files Mini Filter Driver (CVE-2024-30085)
- Windows Process Activation (CVE-2025-21204)
- Windows Update Service (CVE-2025-48799)
- Linux Kernel (CVE-2025-38001)

Code Injection (1)

- Django (CVE-2025-64459)

Other Vulnerabilities (4)

Arbitrary File Reading (1)

- TrueConf Server (BDU:2025-10115)

Remote Code Execution (2)

Отечественные продукты

4 трендовые RCE уязвимости:

- CommuniGate Pro (BDU:2025-01331)
- TrueConf Server (цепочка BDU:2025-10114, BDU:2025-10115, BDU:2025-10116)

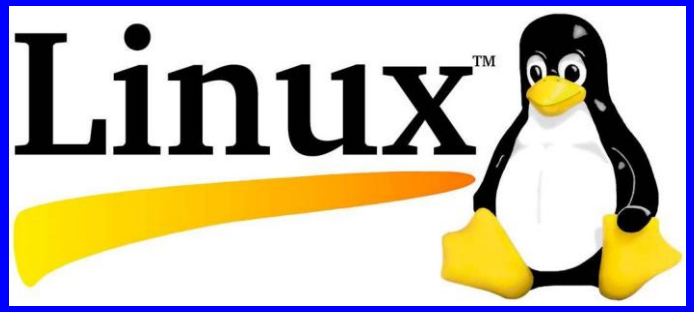
30 трендовых уязвимостей касаются продуктов Microsoft (47%):

- 17 EoP в ядре Windows и стандартных компонентах
- 2 RCE в Microsoft SharePoint
- 2 RCE в стандартных компонентах Windows, эксплуатирующаяся через взаимодействие с сетевым хостом (WSUS, LDAP)
- 9 RCE, Spoofing, SFB в стандартных компонентах Windows, которые могут эксплуатироваться в фишинговых атаках

Ещё фишинг

8 трендовых уязвимостей:

- RCE в архиваторе 7-Zip (BDU:2025-01793, CVE-2025-04116, CVE-2025-55188), архиваторе WinRAR (CVE-2025-6218, CVE-2025-8088)
- XSS в MDaemon Email Server (CVE-2024-11182), Zimbra Collaboration (CVE-2024-27443, CVE-2025-27915)



2 трендовые уязвимости повышения привилегий:

- Sudo (CVE-2025-32463)
- Linux Kernel (CVE-2025-38001)

Библиотеки и фреймворки

2 трендовые уязвимости:

- RCE в expr-eval (CVE-2025-12735)
- XSS в Django (CVE-2025-64459)

JavaScript Expression Evaluator

npm v2.0.2 cdnjs v2.0.2 build unknown

django

Сетевая безопасность

13 трендовых уязвимостей, которые могут являться точками проникновения злоумышленников

- RCE в Cisco ASA и FTD (цепочка CVE-2025-20362, CVE-2025-20333), CommuniGate Pro (BDU:2025-01331), TrueConf Server (цепочка BDU:2025-10114, BDU:2025-10115, BDU:2025-10116), Roundcube (CVE-2025-49113), XWiki Platform (CVE-2025-24893), Control Web Panel (CVE-2025-48703), Redis (CVE-2025-49844) и Erlang/OTP (CVE-2025-32433)
- Authentication Bypass в FortiOS (CVE-2024-55591) и PAN-OS (CVE-2025-0108)

Разработка ПО

2 трендовые RCE уязвимости

- Apache HTTP Server (CVE-2024-38475)
- Apache Tomcat (CVE-2025-24813)

Виртуальная инфраструктура

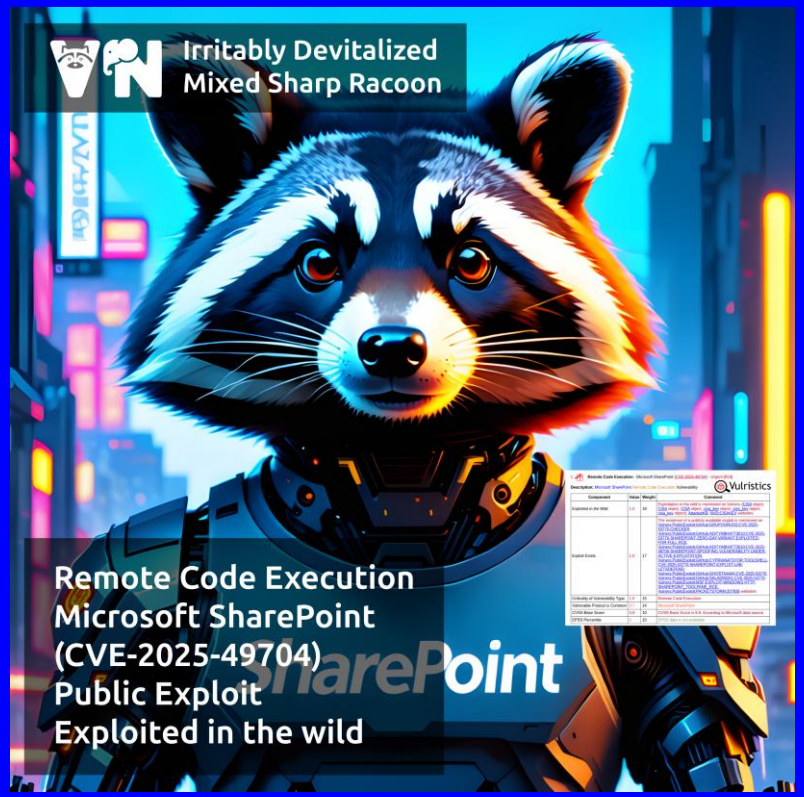
4 трендовые уязвимости:

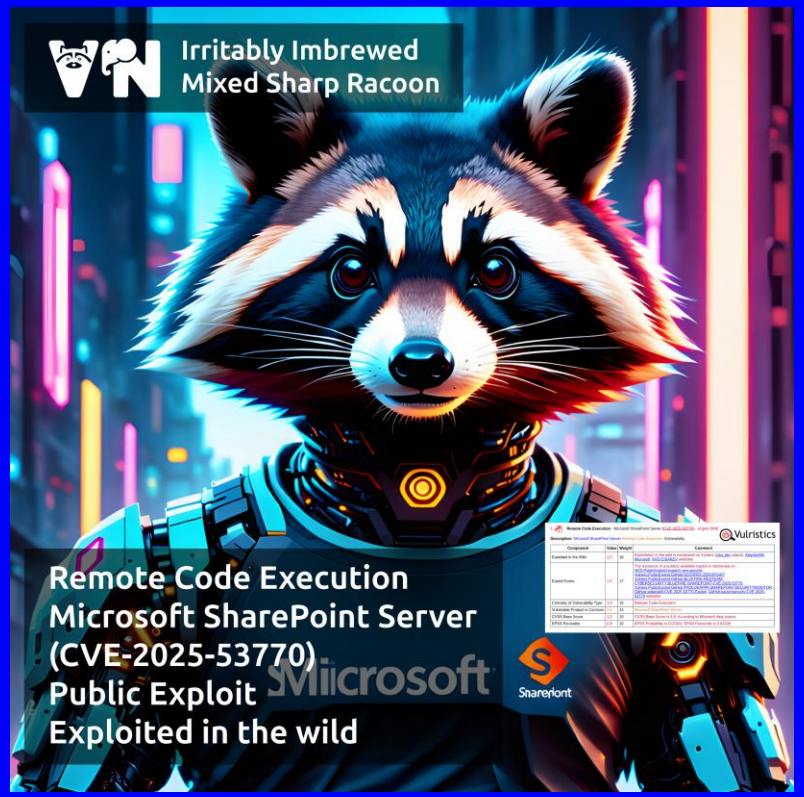
- RCE в ESXi (CVE-2025-22224) и Kubernetes (CVE-2025-1974)
- Information Disclosure в ESXi (CVE-2025-22226)
- Memory Corruption в ESXi (CVE-2025-22225)

ERP

2 трендовые уязвимости в SAP NetWeaver (CVE-2025-31324, CVE-2025-42999)

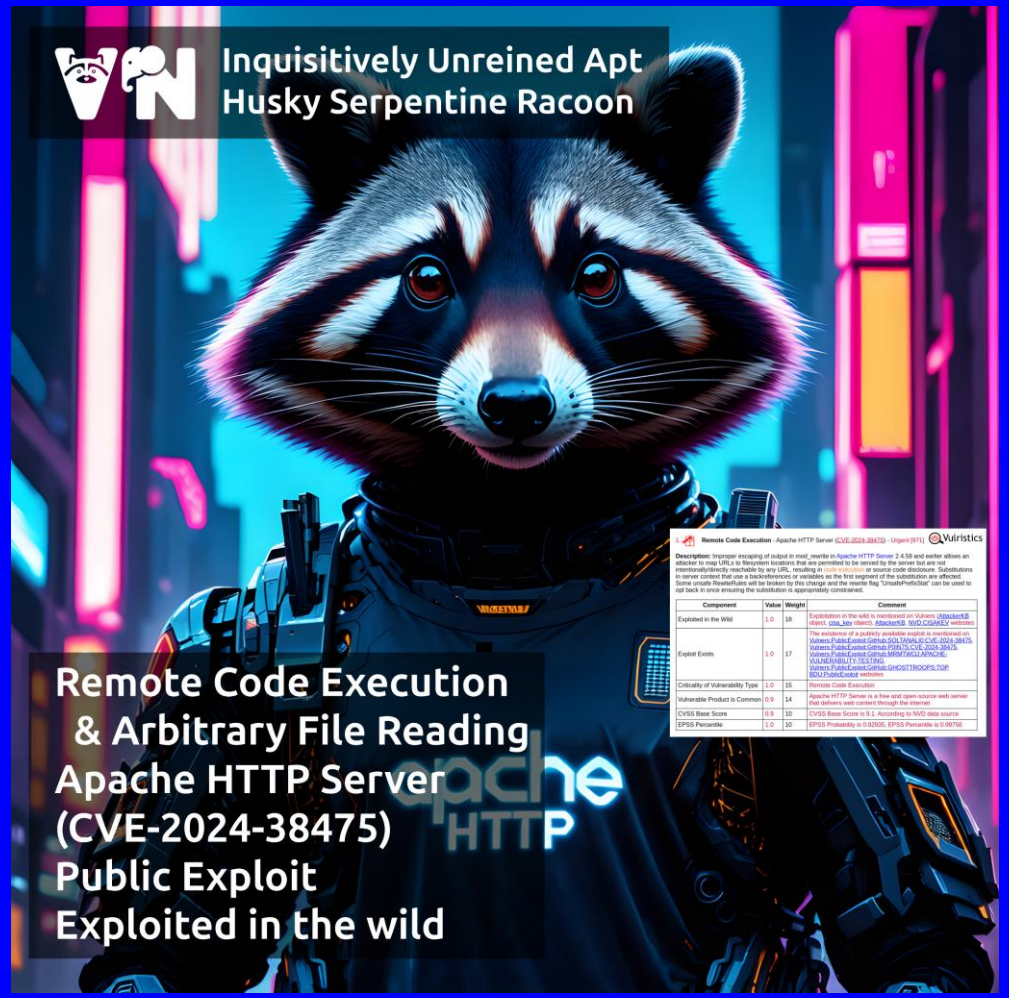
Наиболее интересные (1)





Наиболее интересные (2)

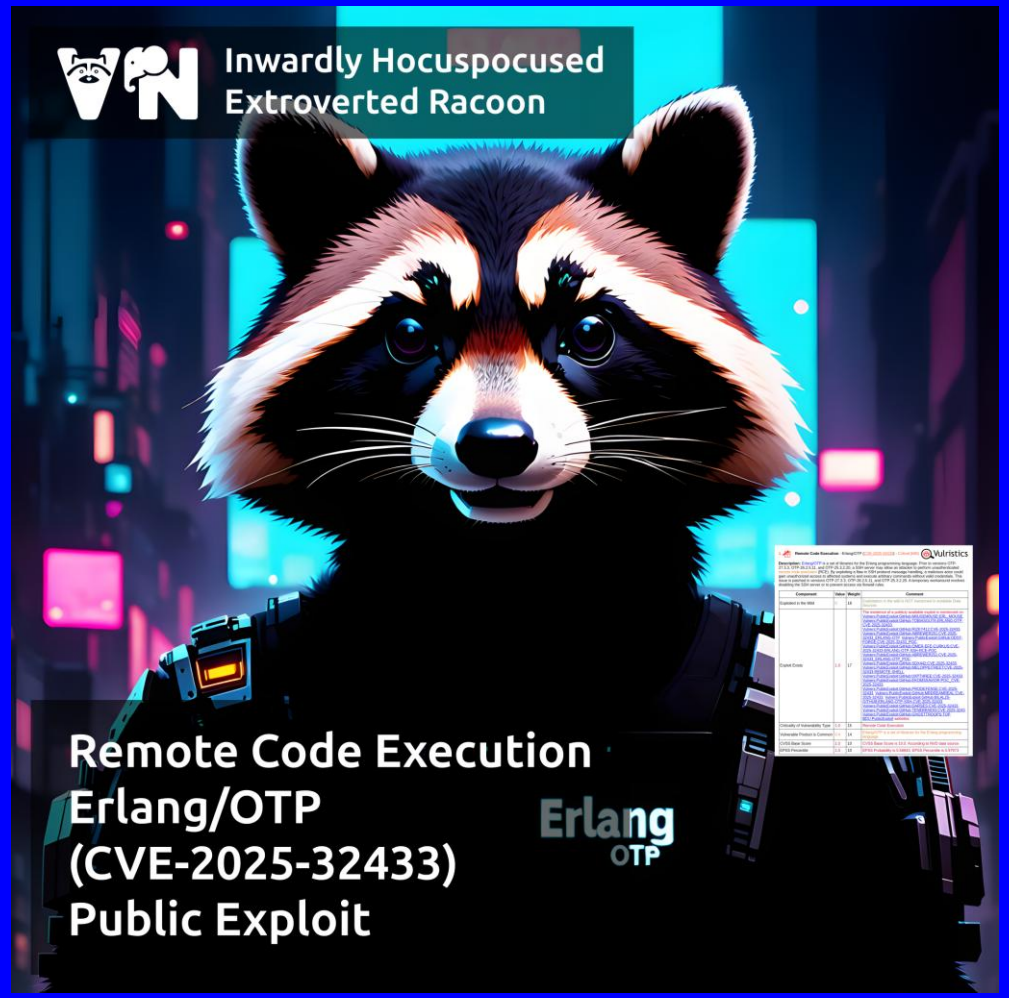
Наиболее интересные (3)



Эксплуатируется вживую на шлюзах безопасного доступа SonicWall SMA, но скорее всего не только...

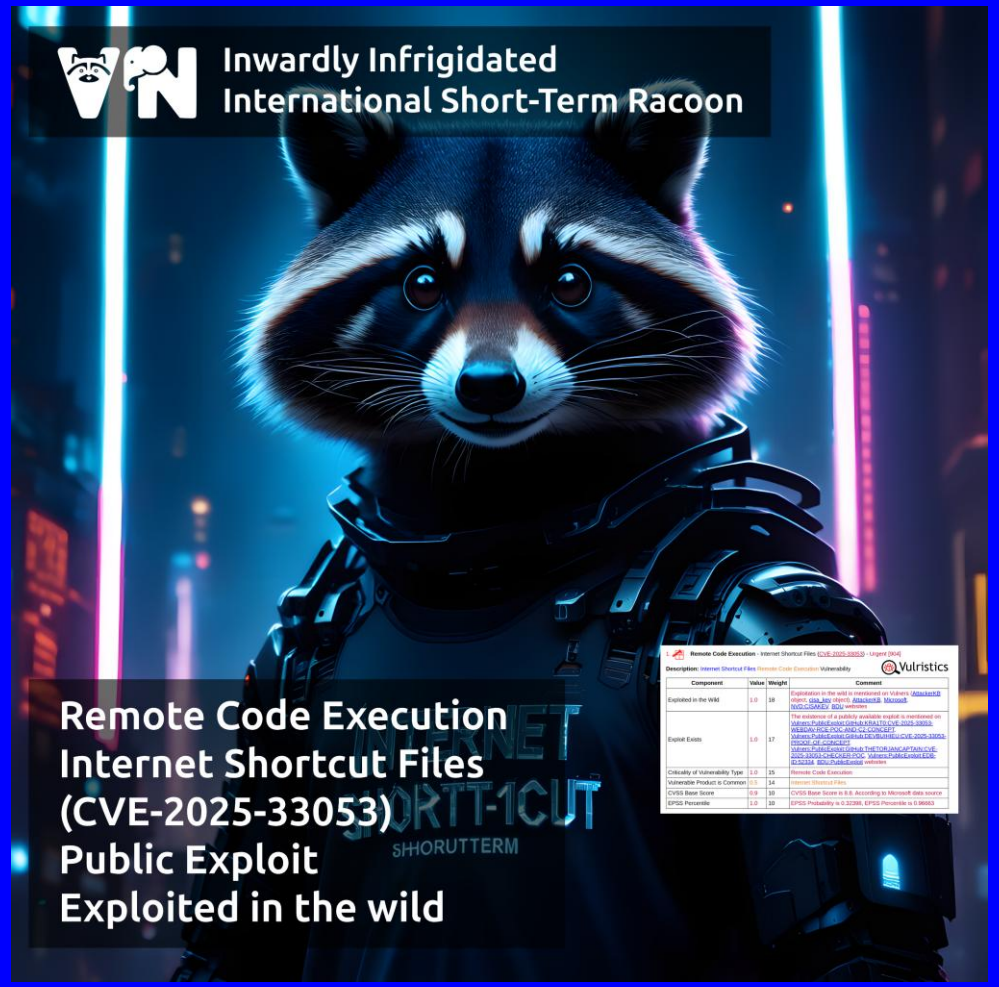
Наиболее интересные (4)

Используется в телекоммуникациях, банковской сфере, e-commerce, компьютерной телефонии и мессенджерах



Уязвимости подвержены устройства Cisco.
И, наверняка, не только они…

Наиболее интересные (5)



...при открытии жертвой специального .url-файла

Когда файловый менеджер Windows видит в папке файл типа .library-ms, он автоматически начинает его парсить

Прогноз на 2026

- От Microsoft ожидаем примерно столько же трендовых.
- По западным сетевым устройствам ожидаем снижения, т.к. импортозамещение идёт и их влияние на отечественный IT-ландшафт снижается.
- Ожидаем появление трендовых уязвимостей в отечественном ПО, т.к. его доля растёт и есть многочисленные акторы заинтересованные в их ресёрче и эксплуатации.
- Трендовыми будут чаще становиться уязвимости активов, которые доступны на периметре и особенно веб-приложений.

Что делать?

- Развивать VM-процесс, **приоритизировано устранять** уязвимости, обращая внимание на трендовые уязвимости. О других уязвимостях тоже не забывайте, они могут со временем стать трендовыми.
- При выборе VM-решений обращать внимание на то, какие уязвимости они умеют детектировать и как быстро добавляют правила детектирования.

СПАСИБО ЗА ВНИМАНИЕ!

t.me/avleonovrus

АЛЕКСАНДР
ЛЕОНОВ