КОД ИБ

ИТОГИ

УЯЗВИМОСТИ 2024

АЛЕКСАНДР ЛЕОНОВ
Ведущий эксперт PT Expert Security Center
Positive Technologies

КОД ИБ
ИТОГИ

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

КОД ИБ

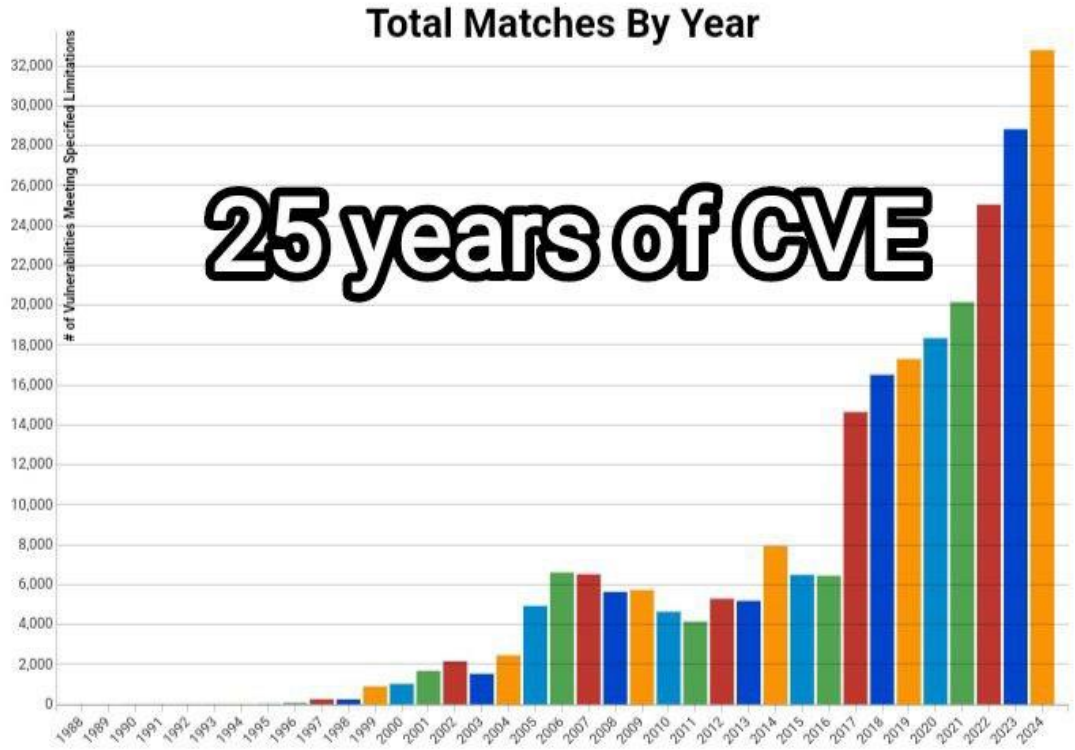
ИТОГИ

NVD

Below are a table and graphs with data matching the characteristics you specified on the Statistics Query Page.

Search Parameters:

- Results Type: Statistics
- Search Type: Search All
- CPE Name Search: false



Количество CVE перевалило за 250 000 идентификаторов (без Rejected).

Количество новых CVE каждый год ставит рекорды, в этом году ожидается больше 35 000.

КОД ИБ
ИТОГИ

NVD

Беклог на анализ больше 20000!

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

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

КОД ИБ
ИТОГИ

Трендовые уязвимости

Трендовые уязвимости — это уязвимости, которые активно используются в атаках или с высокой степенью вероятности будут использоваться в ближайшее время.

NVD

> 35 000

Трендовые

70

КОД ИБ
ИТОГИ

В тренде VM

Управление Уязвимостями и прочее > Плейлисты > В Тренде VM

В тренде VM: топ уязвимостей октября, «метод Форда» и «атака на жалобщика»
SecurityLab
4,6 тыс просмотров · 14 дней назад

9 роликов

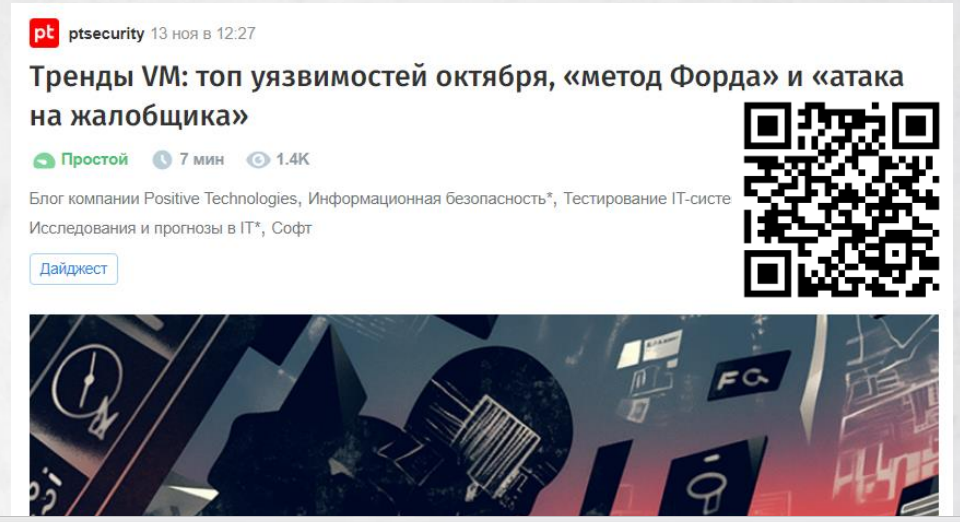
В тренде VM: уязвимости сентября
SecurityLab
5,4 тыс просмотров · 1 месяц назад

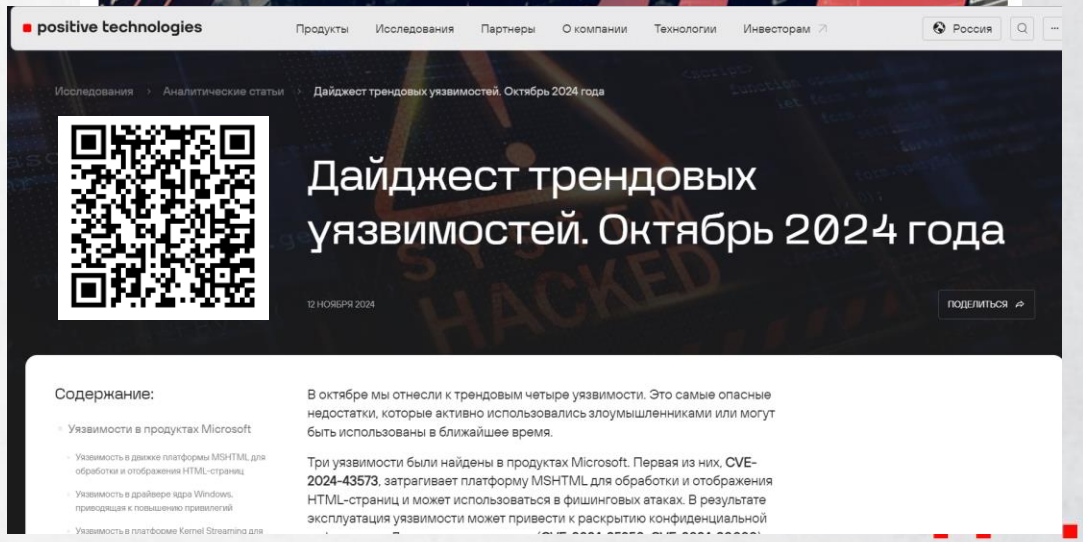
В тренде VM: дайджест за август
SecurityLab
2,7 тыс просмотров · 2 месяца назад

В Тренде VM Июль 2024: 3 CVE в Windows, Artifex Ghostscript, и Acronis Cyber Infrastructure
Управление Уязвимостями и прочее
285 просмотров · 3 месяца назад

В Тренде VM Июнь 2024: 9 CVE в Windows, PHP, Linux, Check Point, VMware vCenter и Veeam
Управление Уязвимостями и прочее
56 просмотров · 3 месяца назад

В Тренде VM Май 2024: 4 CVE в Fluent Bit, Confluence и Windows
Управление Уязвимостями и прочее
12 просмотров · 3 месяца назад





КОД ИБ

ИТОГИ

https://avleonov.com/vulristics_reports/pt_trend_cve_combined2024_report_with_comments_ext_img.html

Vulristics

Report Name: pt_trend_cve_combined2024 report
Generated: 2024-12-04 18:21:31

Vulristics Vulnerability Scores

- All vulnerabilities: 70
- Urgent: 38
- Critical: 21
- High: 11
- Medium: 0
- Low: 0

Basic Vulnerability Scores

- All vulnerabilities: 70
- Critical: 30
- High: 32
- Medium: 8
- Low: 0

Products

Product Name	Prevalence	U	C	H	M	L	A	Comment
GitLab	0.9	1					1	GitLab is a DevOps software package that combines the ability to develop, secure, and operate software in a single application
Windows Kernel	0.9	2	1				3	Windows Kernel
nftables	0.9	1					1	nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames
Juniper JunOS	0.8		1				1	Junos OS is a FreeBSD-based network operating system used in Juniper Networks routing, switching and security devices
Microsoft Exchange	0.8	1	1				2	Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft
PHP	0.8	1					1	PHP is a general-purpose scripting language geared towards web development. It was originally created by Danish-Canadian programmer Rasmus Lerdorf in 1993

Vulnerability Types

Vulnerability Type	Criticality	U	C	H	M	L	A
Remote Code Execution	1.0	12	6	3			21
Authentication Bypass	0.98	7		1			8
Code Injection	0.97	1	1				2
Command Injection	0.97	2					2
Security Feature Bypass	0.9	5	2				7
Elevation of Privilege	0.85	9	5	5			19
Information Disclosure	0.83	1	1				2
Cross Site Scripting	0.8	1					1
Path Traversal	0.7			1			1
Memory Corruption	0.5		1				1
Spoofing	0.4		5	1			6

12. **Remote Code Execution** - FortiClientEMS (CVE-2023-48788) - Urgent [916]

Description: A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.

Component	Value	Weight	Comment
Exploited in the Wild	1.0	18	Exploitation in the wild is mentioned on Vulners (AttackerKB object, cisa_kev object), AttackerKB, BDU websites
Exploit Exists	1.0	17	The existence of a publicly available exploit is mentioned on Vulners:PublicExploit:GitHub:HORIZON3AI:CVE-2023-48788, Vulners:PublicExploit:MSF:EXPLOIT-WINDOWS-HTTP-FORTICLIENT_EMS_FCTID_SQLI-, Vulners:PublicExploit:1337DAY-ID-39585, Vulners:PublicExploit:PACKETSTORM:178230 websites
Criticality of Vulnerability Type	1.0	15	Remote Code Execution
Vulnerable Product is Common	0.5	14	FortiClient EMS provides efficient and effective administration of endpoints running FortiClient (a Fabric Agent that delivers protection, compliance, and secure access in a single, modular lightweight client)
CVSS Base Score	1.0	10	CVSS Base Score is 9.8. According to Vulners data source
EPSS Percentile	1.0	10	EPSS Probability is 0.71085, EPSS Percentile is 0.9816

КОД ИБ

ИТОГИ

Exploitation in the wild detected (52)

Authentication Bypass (7)

- GitLab (CVE-2023-7028)
- TeamCity (CVE-2024-27198)
- Jenkins (CVE-2024-23897)
- Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21893)
- Acronis Cyber Infrastructure (CVE-2023-45249)
- PAN-OS (CVE-2024-0012)

Remote Code Execution (12)

- PHP (CVE-2024-4577)
- Atlassian Confluence (CVE-2023-22527)
- PaperCut NG (CVE-2023-27350)
- Windows MSHTML Platform (CVE-2023-35628)
- FortiClientEMS (CVE-2023-48788)
- FortiManager (CVE-2024-47575)
- PAN-OS (CVE-2024-3400)

Public exploit exists, but exploitation in the wild is NOT detected (16)

Remote Code Execution (7)

- Juniper JunOS (CVE-2024-21591)
- Atlassian Confluence (CVE-2024-21683)
- Windows Remote Desktop Licensing Service (CVE-2024-38077)
- XWiki Platform (CVE-2024-31982)
- Microsoft Outlook (CVE-2024-21413)
- FortiOS (CVE-2023-42789)
- Fluent Bit (CVE-2024-4323)

Elevation of Privilege (6)

- Windows Common Log File System Driver (CVE-2023-36424)
- Windows CSC Service (CVE-2024-26229)

Other Vulnerabilities (2)

Remote Code Execution (2)

- VMware vCenter (CVE-2024-37079, CVE-2024-37080)

КОД ИБ

ИТОГИ

Exploitation in the wild detected (52)

Authentication Bypass (7)

- GitLab (CVE-2023-7028)
- TeamCity (CVE-2024-27198)
- Jenkins (CVE-2024-23897)
- Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21893)
- Acronis Cyber Infrastructure (CVE-2023-45249)
- PAN-OS (CVE-2024-0012)

Remote Code Execution (12)

- PHP (CVE-2024-4577)
- Atlassian Confluence (CVE-2023-22527)
- PaperCut NG (CVE-2023-27350)
- Windows MSHTML Platform (CVE-2023-35628)
- FortiClientEMS (CVE-2023-48788)
- FortiManager (CVE-2024-47575)
- PAN-OS (CVE-2024-3400)

Public exploit exists, but exploitation in the wild is NOT detected (16)

Remote Code Execution (7)

- Juniper JunOS (CVE-2024-21591)
- Atlassian Confluence (CVE-2024-21683)
- Windows Remote Desktop Licensing Service (CVE-2024-38077)
- XWiki Platform (CVE-2024-31982)
- Microsoft Outlook (CVE-2024-21413)
- FortiOS (CVE-2023-42789)
- Fluent Bit (CVE-2024-4323)

Elevation of Privilege (6)

- Windows Common Log File System Driver (CVE-2023-36424)
- Windows CSC Service (CVE-2024-26229)

Other Vulnerabilities (2)

Remote Code Execution (2)

- VMware vCenter (CVE-2024-37079, CVE-2024-37080)

КОД ИБ
ИТОГИ

Пример предсказания

VMware vCenter (CVE-2024-38812)

- добавлена в список трендовых 20 сентября, через 3 дня после появления бюллетеня безопасности вендора
- признаки эксплуатации появились только через 2 месяца, 18 ноября

КОД ИБ

ИТОГИ

Январское «выравнивание»

- Barracuda Email Security Gateway (CVE-2023-2868)
- MOVEit Transfer (CVE-2023-34362)
- papercut (CVE-2023-27350)
- SugarCRM (CVE-2023-22952)

КОД ИБ

ИТОГИ

Отечественных нет

Все эти уязвимости в западных коммерческих продуктах и open source проектах.

КОД ИБ
ИТОГИ

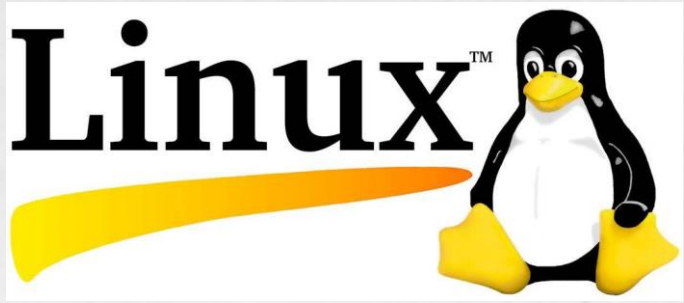
Microsoft

32 трендовых уязвимостей в продуктах Microsoft (45 %)

- Из них 15 уязвимостей повышения привилегий в ядре Windows и стандартных компонентах
- Из них 1 уязвимость выполнения произвольного кода Windows в Remote Desktop Licensing Service (CVE-2024-38077)

КОД ИБ

ИТОГИ



2 трендовые уязвимости касаются повышения привилегий в Linux:

- nftables (CVE-2024-1086)
- needrestart (CVE-2024-48990)

КОД ИБ

ИТОГИ

19 могут использоваться в фишинговых атаках

Windows

Outlook

Exchange

roundcube
open source webmail software

13 ставят под угрозу сетевую безопасность организации и могут являться точками проникновения злоумышленников

paloalto NETWORKS

FORTINET

JUNIPER NETWORKS

CHECK POINT

ivanti

ZYXEL NETWORKS

7 позволяют злоумышленникам скомпрометировать виртуальную инфраструктуру и бэкапы организации

vmware

VEEAM Backup & Replication

КОД ИБ

ИТОГИ

5 позволяют злоумышленникам скомпрометировать ПО, разрабатываемое в компании

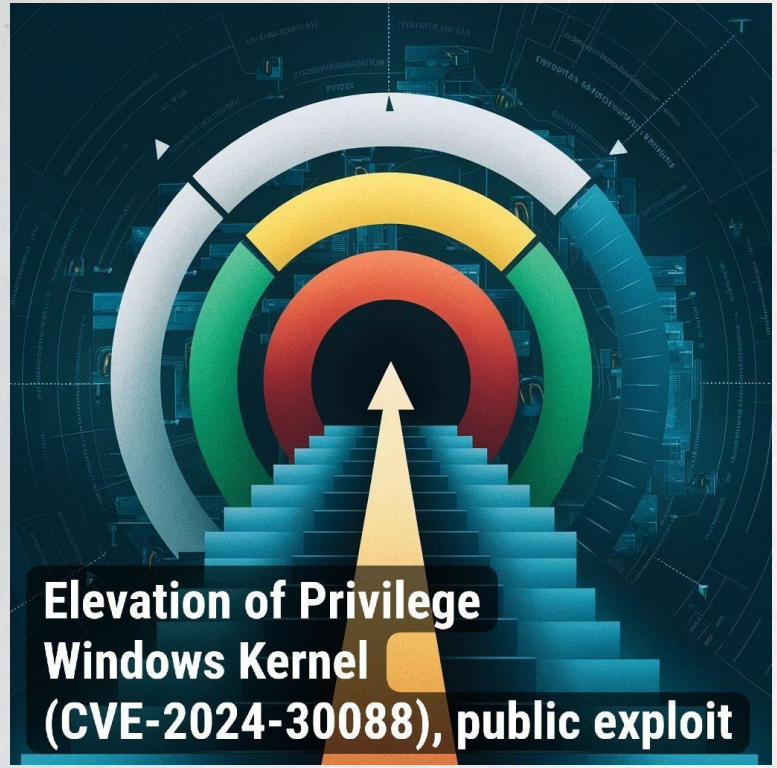
3 могут использоваться в атаках на инструменты совместной работы

2 в плагинах CMS WordPress

КОД ИБ

ИТОГИ

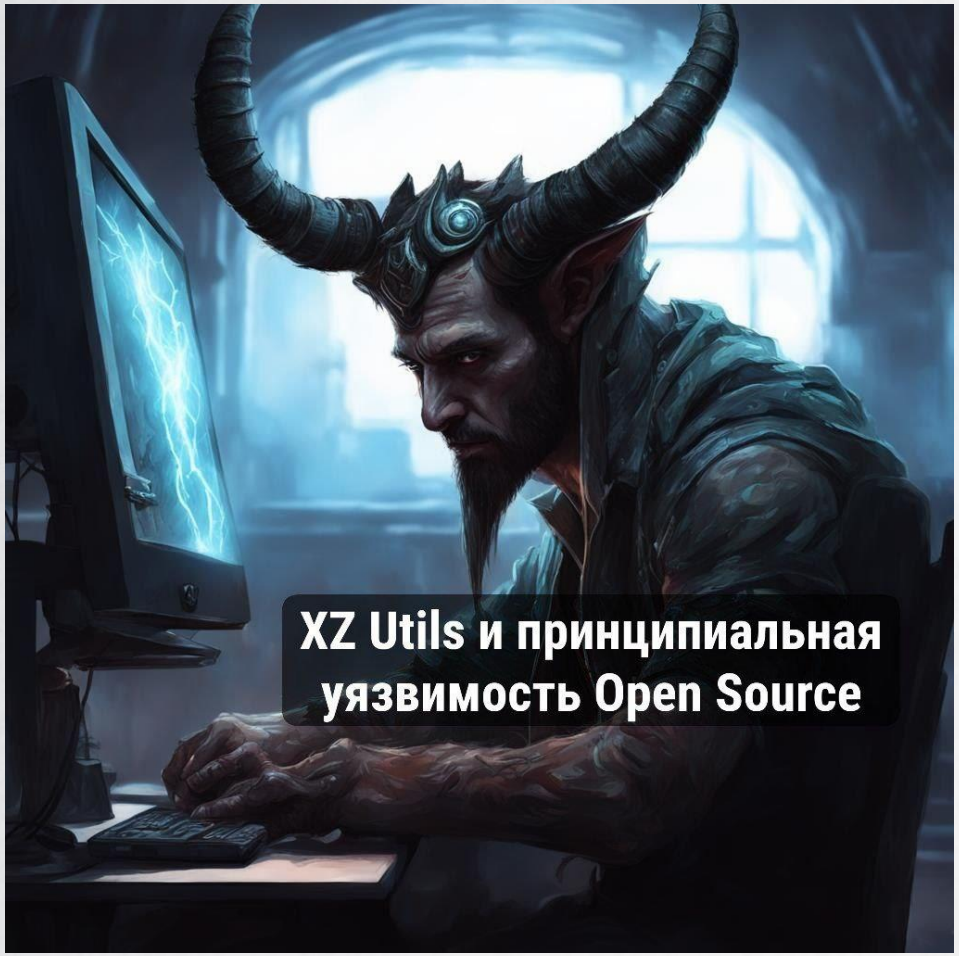
Мой топ наиболее типичных



КОД ИБ

ИТОГИ

Не уязвимости, но важно



КОД ИБ

ИТОГИ

Что будет в 2025?

- От Microsoft ожидаем примерно столько же
- 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.

КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!

t.me/avleonovrus

АЛЕКСАНДР
ЛЕОНОВ