




ТРЕНДОВЫЕ УЯЗВИМОСТИ 2023: ПОЧЕМУ ВАЖНО И ПОЧЕМУ ТРУДНО?

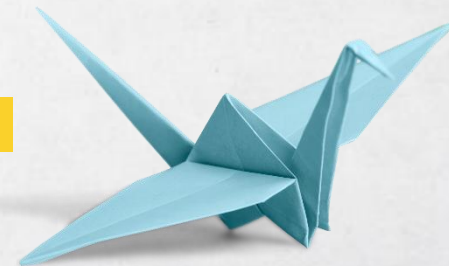


О СЕБЕ

- Леонов Александр
- Занимаюсь в VULNERABILITY MANAGEMENT-ом с 2009
- Сейчас работаю в  **VM вендоре**
- Веду Telegram-канал

"Управление Уязвимостями и прочее"

[T.ME/AVLEONOVVRUS](https://t.me/AVLEONOVVRUS)



ТРЕНДОВЫЕ УЯЗВИМОСТИ: ЧТО ЭТО И ЗАЧЕМ?

Базы уязвимостей

2023

NVD

25998



БДУ ФСТЭК

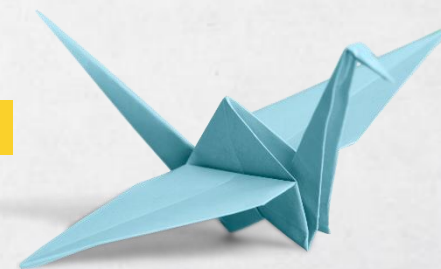
6341



трендовые
уязвимости

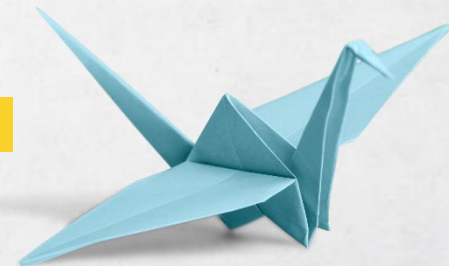
105

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



ЧТО ВЛИЯЕТ НА ТРЕНДОВОСТЬ УЯЗВИМОСТИ

- Может быть использована злоумышленником для **развития атаки** на инфраструктуру и реализации **недопустимого события**
- Есть **эксплоит** (желательно публичный и проверенный)
- В **распространенном** продукте

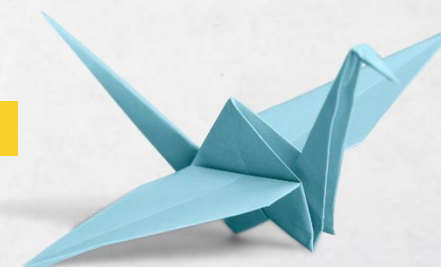
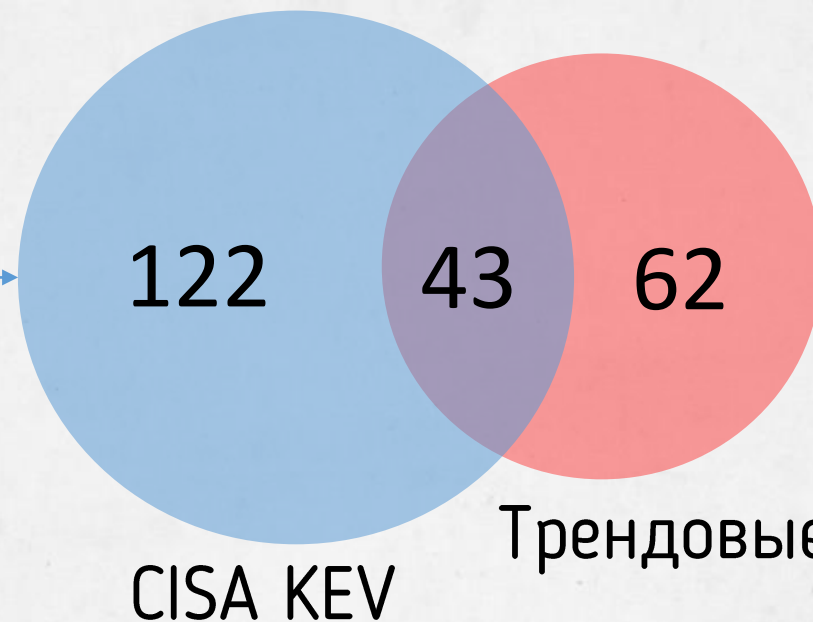


ПОЧЕМУ НЕДОСТАТОЧНО CISA KEV?

Релевантность

2023

Некритичные/
неактуальные



ПОЧЕМУ НЕДОСТАТОЧНО CISA KEV?

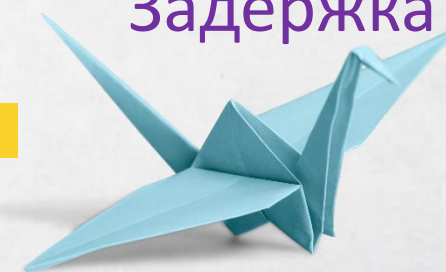
Задержки



Remote Code Execution ([CVE-2023-36844](#),
[CVE-2023-36845](#), [CVE-2023-36846](#),
[CVE-2023-36847](#))



- Об уязвимостях стало известно в **середине августа**.
- 25 августа Shadowserver сообщили о уязвимостей вживую.
- В трендовых с **28 августа**.
- В CISA KEV эти уязвимости добавили только **13 ноября**.
Задержка ~ 3 месяца



ПОЧЕМУ НЕДОСТАТОЧНО CISA KEV?

Задержки



Elevation of Privilege в
Linux GNU C library ([CVE-2023-4911](#))



- Об уязвимости стало известно **3 октября**.
- Публичный PoC эксплоит для неё был готов уже на следующий день.
- В трендовых **4 октября**.
- В начале ноября уязвимость начала эксплуатироваться в [зловреде Kinsing](#).
- В CISA KEV уязвимость появилась только **21 ноября**.

Задержка ~ 1,5 месяца



ПОЧЕМУ НЕДОСТАТОЧНО CISA KEV?

Причины задержек

GNU | GNU C LIBRARY



[CVE-2023-4911](#)

GNU C Library Buffer Overflow Vulnerability

GNU C Library's dynamic loader ld.so contains a buffer overflow vulnerability when processing the GLIBC_TUNABLES environment variable, allowing a local attacker to execute code with elevated privileges.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2023-11-21
- **Due Date:** 2023-12-12

[Resources and Notes +](#)




Events that do not constitute as active exploitation, in relation to the KEV catalog, include:

- Scanning
- Security research of an exploit
- Proof of Concept (PoC)

ПОЧЕМУ НЕДОСТАТОЧНО CISA KEV?

Причины задержек

GNU | GNU C LIBRARY

 [CVE-2023-](#)

GNU C Library Buffer Overflow

GNU C Library's dynamic environment variables

- **Action:** Apply mitigation to the product if mitigations are available.
- **Known To Be Unaffected:** None.
- **Date Added:** 2023-08-01
- **Due Date:** 2023-08-01

[Resources and Notes](#)



..., in relation to the KEV catalog, include:

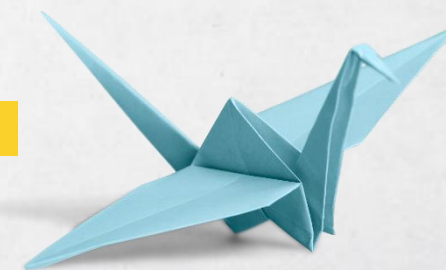
- Proof of Concept (PoC)

ПОЧЕМУ НЕДОСТАТОЧНО ЭКСПЛОИТОВ ИЗ NVD?

- ТОЛЬКО 26 ИЗ 105 ТРЕНДОВЫХ УЯЗВИМОСТЕЙ, ИМЕЛИ ПУБЛИЧНЫЕ ССЫЛКИ НА ЭКСПЛОИТ В NVD.

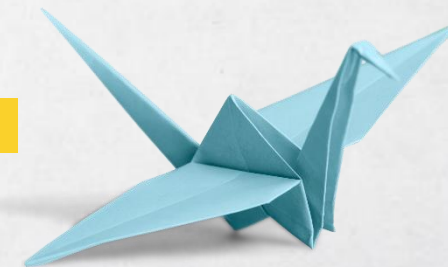


Hyperlink	Resource
http://packetstormsecurity.com/files/174986/glibc-ld.so-Local-Privilege-Escalation.html	
http://seclists.org/fulldisclosure/2023/Oct/11	
http://www.openwall.com/lists/oss-security/2023/10/03/2	Exploit Mailing List
http://www.openwall.com/lists/oss-security/2023/10/03/3	Mailing List Patch
http://www.openwall.com/lists/oss-security/2023/10/05/1	Mailing List Third Party Advisory



ИЗМЕНЕНИЕ ОПИСАНИЯ УЯЗВИМОСТИ

- AUTHENTICATION BYPASS УЯЗВИМОСТЬ В ATlassian CONFLUENCE (CSC-2023-22518)
- В МОМЕНТ ВЫХОДА БЮЛЛЕТЕНЯ БЕЗОПАСНОСТИ:
«ЗЛОУМЫШЛЕННИК НЕ СМОЖЕТ НАРУШИТЬ КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ»
- ЧЕРЕЗ НЕДЕЛЮ:
«ЗЛОУМЫШЛЕННИК С ПОМОЩЬЮ ЭТОЙ УЯЗВИМОСТИ **МОЖЕТ ПОЛУЧИТЬ ПРАВА АДМИНИСТРАТОРА**»



НЕСТАНДАРТНЫЕ CVE УЯЗВИМОСТИ

- SUPPLY CHAIN АТАКА С ИСПОЛЬЗОВАНИЕМ ЗАТРОЯНЕННОГО ПРИЛОЖЕНИЯ 3CX DESKTOPAPP ([CVE-2023-29059](#))

Description

3CX DesktopApp through 18.12.416 has embedded malicious code, as exploited in the wild in March 2023. This affects versions 18.12.407 and 18.12.416 of the 3CX DesktopApp Electron Windows application shipped in Update 7, and versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 of the 3CX DesktopApp Electron macOS application.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Weakness Enumeration

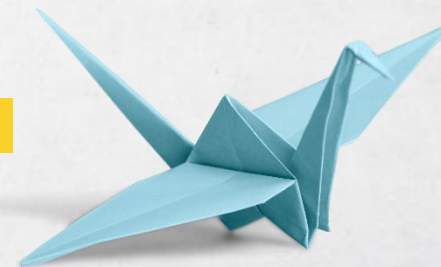
CWE-ID

NVD-CWE-noinfo

CWE Name

Insufficient Information

- RCE?



CVE УЯЗВИМОСТИ, КОТОРЫХ НЕТ В NVD



← ↻ 🏠 🔒 https://www.rarlab.com/vu... 🔍 🗨️ ☆ 📄

Introduction

We have received many questions from software developers and WinRAR users about the CVE-2023-40477 vulnerability. We would like to provide more details here.

Description

A buffer overflow is possible when processing recovery volume names in the old RAR 3.0 format. The user must start unpacking a RAR file in the same folder as a REV file with a malformed name to trigger this vulnerability. This has been fixed in WinRAR 6.23.



× 🏠 🔒 https://xakep.ru/2023/10/02/exim-rce-problems/ 🔍 ☆ 📄 🗨️ 📄 🗨️

Ситуация усугубляется тем, что Exim используют сотни тысяч или даже миллионы почтовых серверов по всему миру. Так, согласно данным [Security Space](#), Exim установлен более чем на 56% почтовых серверов (342 337), обнаруженных в интернете. По информации [Shodan](#), в мире и вовсе насчитывается более 3,5 млн серверов с Exim на борту.

Уязвимость [CVE-2023-42115](#) (9,8 балла по шкале CVSS) была обнаружена исследователем, который предпочел остаться неизвестным. Проблема связана с out-of-bounds записью в компоненте Exim, который отвечает за аутентификацию, и может использоваться для удаленного выполнения кода или команд на уязвимых серверах.

↻ 🏠 🔒 https://nvd.nist.gov/vuln/detail/CVE-2023-40477 🔍 🔍 🔍 🗨️ ☆ 📄 🗨️

CVE ID Not Found

A vulnerability has been identified, and possibly a CVE has been assigned, why is it not in your database?

Although a CVE ID may have been assigned by either CVE or a CNA, it will not be available in the NVD if it has a status of RESERVED by CVE.

↻ 🏠 🔒 https://nvd.nist.gov/vuln/detail/CVE-2023-42115 🔍 🔍 🔍 🗨️ ☆ 📄 🗨️

CVE ID Not Found

A vulnerability has been identified, and possibly a CVE has been assigned, why is it not in your database?

Although a CVE ID may have been assigned by either CVE or a CNA, it will not be available in the NVD if it has a status of RESERVED by CVE.




БДУ УЯЗВИМОСТИ БЕЗ CVE ИДЕНТИФИКАТОРОВ


[Главная](#) / [Список уязвимостей](#) / BDU:2023-05857


BDU:2023-05857: Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом, позволяющая нарушителю выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть

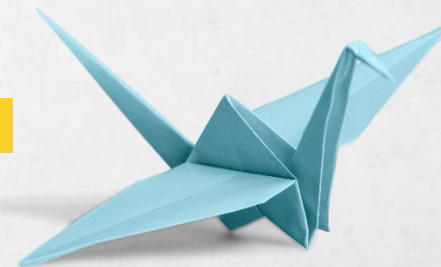
Вид ▾

Описание уязвимости Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть

Вендор  ООО «1С-Битрикс»

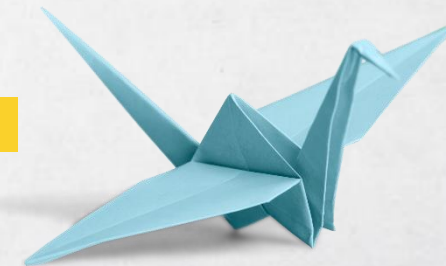
Наименование ПО  1С-Битрикс: Управление сайтом ([запись в едином реестре российских программ №35](#))

Идентификаторы других систем описаний уязвимостей  Данные уточняются



КАК ПРАВИЛЬНО ОПРЕДЕЛЯТЬ ТРЕНДОВЫЕ УЯЗВИМОСТИ?

- АВТОМАТИЗИРОВАНО СОБИРАТЬ И АКТУАЛИЗИРОВАТЬ ИНФОРМАЦИЮ ОБ УЯЗВИМОСТЯХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ
 - БАЗЫ УЯЗВИМОСТЕЙ, БЮЛЛЕТЕНИ БЕЗОПАСНОСТИ ВЕНДОРОВ, СОЦИАЛЬНЫЕ СЕТИ, БЛОГИ, ТЕЛЕГРАММ-КАНАЛЫ, БАЗ ЭКСПЛОИТОВ, ПУБЛИЧНЫХ РЕПОЗИТОРИЕВ КОДА И Т.Д.
- ПРОВОДИТЬ РУЧНУЮ ВЕРИФИКАЦИЮ ИНФОРМАЦИИ
- ПРОГНОЗИРОВАТЬ ТРЕНДОВОСТЬ ЗАРАНЕЕ (В ТОМ ЧИСЛЕ С ПОМОЩЬЮ ML-МОДЕЛИ)



105 ТРЕНДОВЫХ УЯЗВИМОСТЕЙ 2023

REMOTE CODE EXECUTION: 45

ELEVATION OF PRIVILEGE: 22

AUTHENTICATION BYPASS: 15

SECURITY FEATURE BYPASS: 9

COMMAND INJECTION: 3

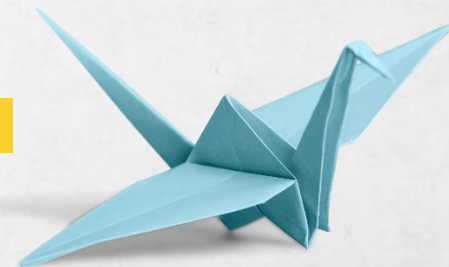
MEMORY CORRUPTION: 3

INFORMATION DISCLOSURE: 3

DENIAL OF SERVICE: 2

PATH TRAVERSAL: 2

CROSS SITE SCRIPTING: 1



105 ТРЕНДОВЫХ УЯЗВИМОСТЕЙ 2023

Корпоративная инфраструктура: 41

Сетевые устройства: 10

Почтовые серверы: 9

Средства совместной работы: 9

ERP и CRM: 4

MDM: 3

Виртуализация: 3

Балансировщики нагрузки: 1

Резервное копирование: 1

Средства мониторинга IT: 1

Операционные системы: 35

Ядро и компоненты Microsoft Windows: 27

Ядро и системные утилиты Linux: 5

Ядро и системные утилиты macOS: 3

Десктопное ПО: 10

Архиваторы: 2

Веб-браузеры: 2

Клиенты для работы с электронной почтой: 2

Текстовые редакторы: 2

Клиенты для работы с IP-телефонией: 1

Программы для просмотра PDF: 1

Разработка приложений: 10

Модули и библиотеки: 5

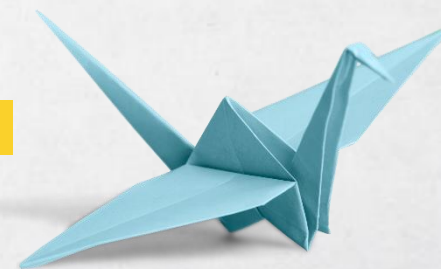
Средства разработки и деплоя: 3

Базы данных и брокеры сообщений: 2


Бизнес-сервисы: 9

CMS и e-commerce: 8

Веб-серверы: 1



ЗАКЛЮЧЕНИЕ

- Трендовые уязвимости – можно выделять самостоятельно, но трудоёмко, т.к. нет достаточно хороших источников по эксплоитам и эксплуатации вживую
- Будет ли полный публичный список трендовых уязвимостей от **VM вендор**  Stay tuned!

