

# S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

**DateLine: 2024-03-12**



LIKE



SUBSCRIBE

S T O R M ⚡ W A T C H



## Storm ⚡ Watch by GreyNoise Intelligence

### GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (<https://www.greynoise.io>), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

<https://StormWatch.ing>




LEAVE A  
COMMENT

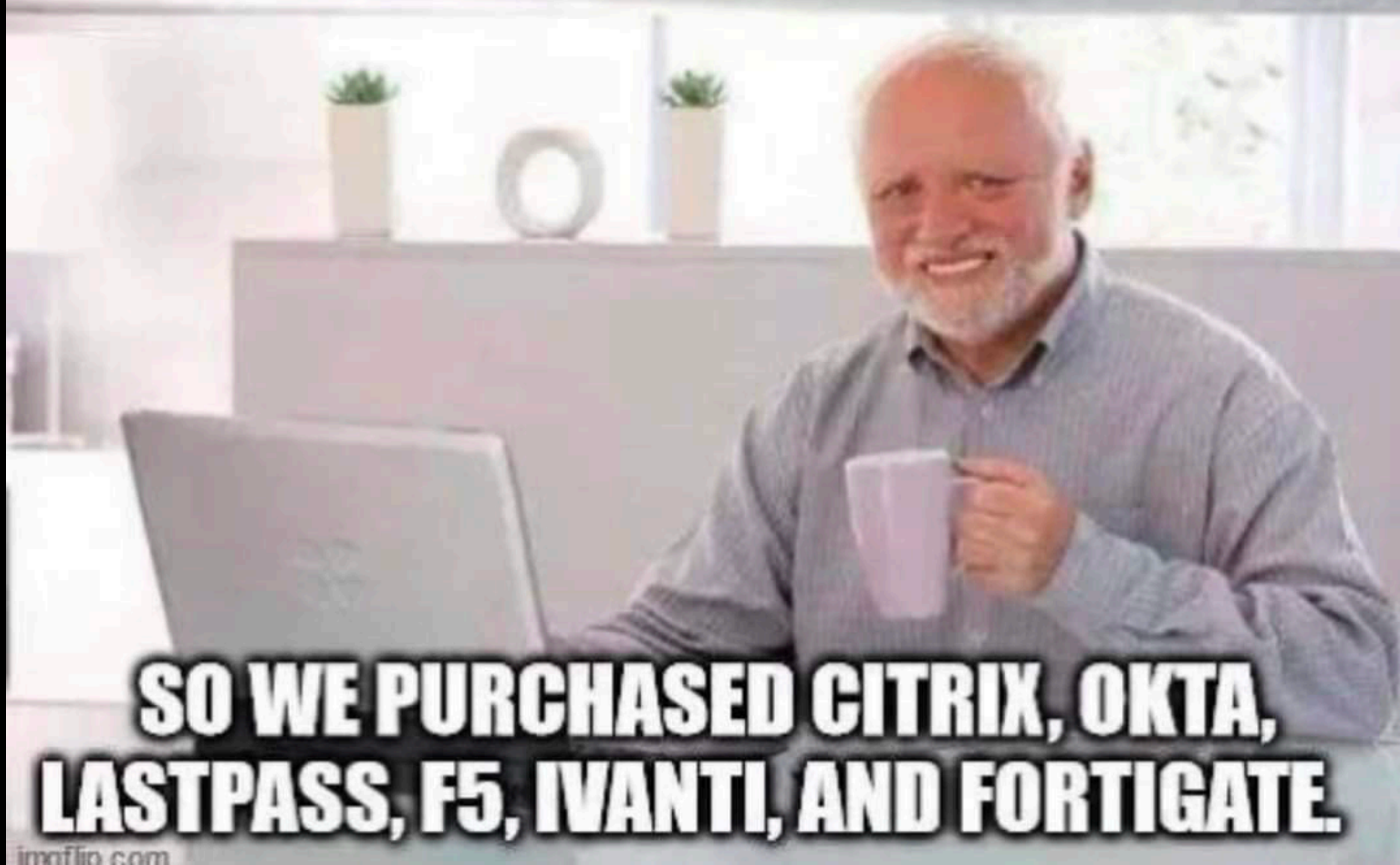


SHARE





**THE CONSULTANTS SAID WE NEEDED  
TO SPEND MORE MONEY ON SECURITY**



**SO WE PURCHASED CITRIX, OKTA,  
LASTPASS, F5, IVANTI, AND FORTIGATE.**



S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

# CYBERSIDE CHAT





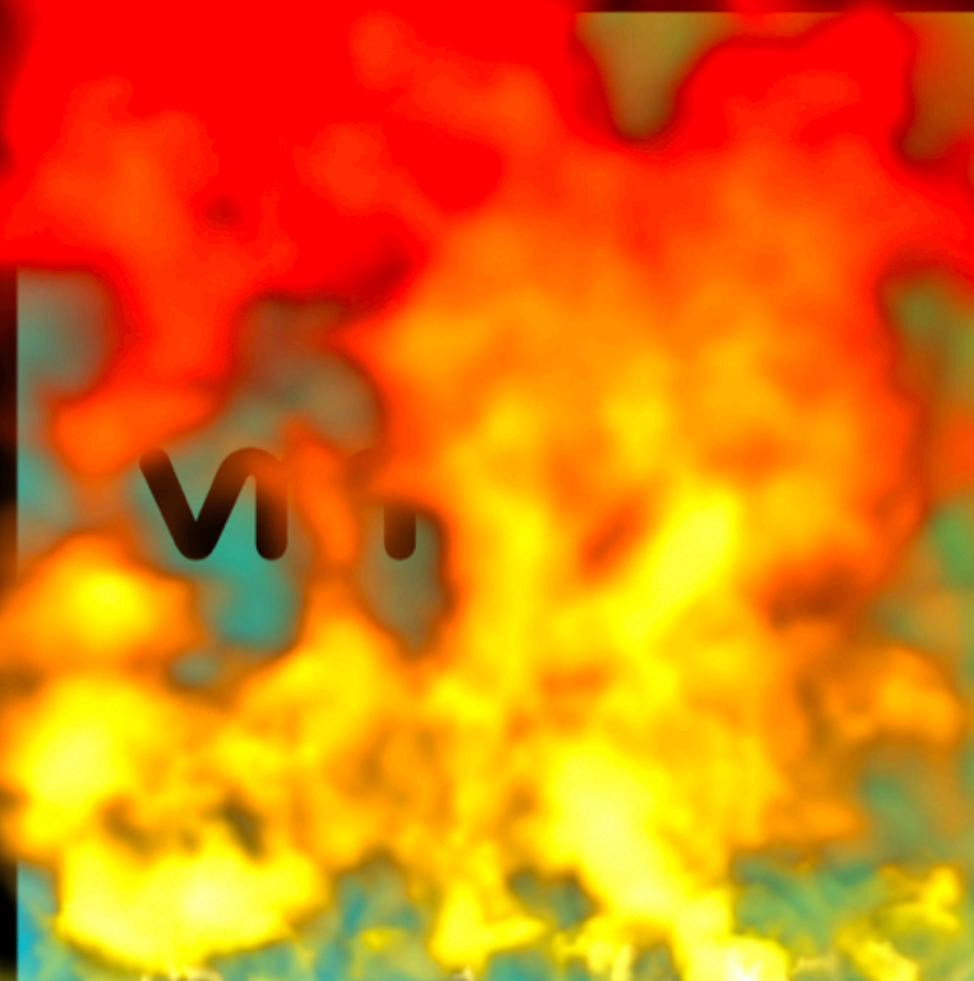
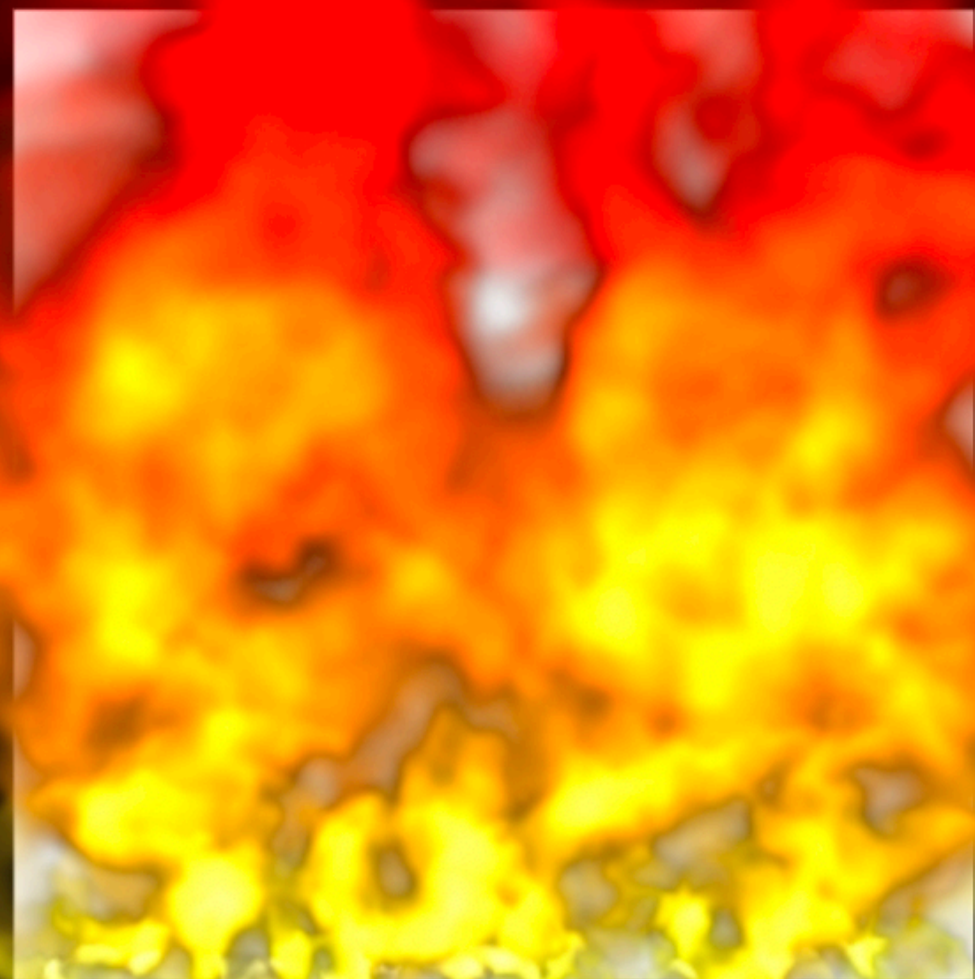
vmware®

vmware®

vmware®

vmware®







VMware has recently addressed a series of critical vulnerabilities: **CVE-2024-22252**, **CVE-2024-22253**, **CVE-2024-22254**, and **CVE-2024-22255**, affecting VMware ESXi, Workstation, Fusion, and Cloud Foundation.

<https://www.securityweek.com/vmware-patches-critical-esxi-sandbox-escape-flaws/>



## CVE-2024-22252 & CVE-2024-22253

Critical use-after-free weaknesses in the XHCI and UHCI USB controllers.

Enable a malicious actor with local administrative privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host.

While on ESXi, the exploitation is contained within the VMX sandbox, on Workstation and Fusion, it could lead to code execution on the host machine itself.



## CVE-2024-22254 & CVE-2024-22255

OOB write weakness in VMware ESXi that could enable a threat actor with VMX process privileges to escape the sandbox.

Information disclosure weakness in the UHCI USB controller that could allow an attacker with administrative access to a virtual machine to leak memory from the vmx process.



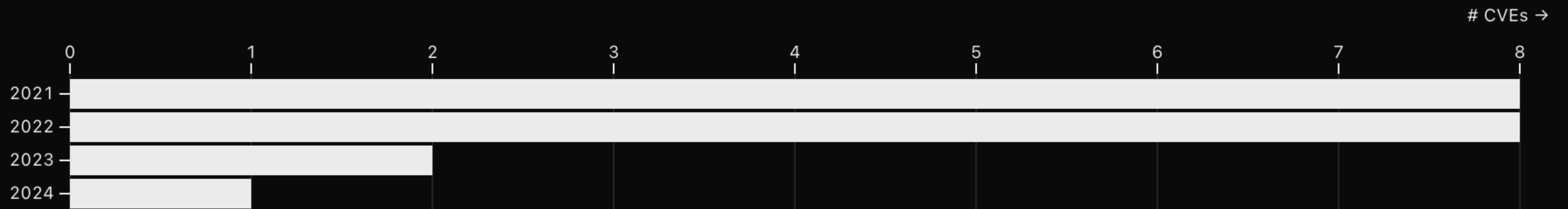
In addition to these vulnerabilities, VMware has also recently urged admins to uninstall a deprecated vSphere plugin that could be exploited for authentication relay and session hijack attacks.

# Vulnerabilities By Vendor

Select Vendor:

VMware

## VMware KEV CVES/Year



VMware: 19 CVEs (👹 = Ransomware | 🛰️ = Remote)

- **VMware vCenter Server Out-of-Bounds Write Vulnerability:** VMware vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol that allows an attacker to conduct remote code execution.

🛰️ CVE: 2023-10-25 • KEV: 2024-01-22 • CVSS: 9.8





239

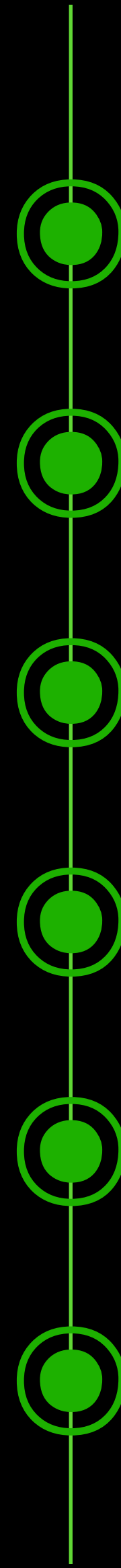


823

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	2	0	1	1	0	5	4	0	0	2
2015	0	0	0	1	0	0	0	0	0	0	4
2016	6	6	0	6	3	2	1	3	0	0	0
2017	10	9	0	8	0	1	2	2	1	0	3
2018	2	4	0	2	3	1	1	0	0	1	2
2019	1	7	0	1	1	0	0	1	0	0	0
2020	2	10	3	5	4	0	1	0	0	1	3
2021	0	1	2	5	4	0	0	0	9	1	2
2022	1	5	1	6	2	0	1	2	1	0	0
2023	1	7	0	1	3	0	1	1	0	2	0
2024	0	2	0	2	0	0	0	0	0	0	0
Total	23	53	6	38	21	4	12	13	11	5	16



Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	8	1
2015	3	1	1	8	0
2016	6	3	3	9	3
2017	20	2	5	12	5
2018	12	2	6	7	8
2019	4	1	3	11	9
2020	14	4	12	15	5
2021	10	6	11	10	16
2022	21	7	17	11	15
2023	10	1	10	12	6
2024	2	2	3	1	4
Total	102	29	71	104	72

- 
- Founded in 1998
  - VMware Workstation released in 1999
  - Acquired by EMC in 2004
  - Dell acquired EMC in 2016
  - Spun off in 2021
  - Acquired by Broadcom in 2023 (\$69b)



S T O R M ⚡ W A T C H

CYBERSECURITY NEWS

# CYBER SPOTLIGHT





Microsoft





# Microsoft: Russians are using stolen information to breach company's systems

Microsoft warned on Friday that Russian hackers behind several headline-grabbing attacks on the U.S. government are now exploiting information they stole from the tech giant's systems in November.

Microsoft's Security Team **said** that in recent weeks, it has seen evidence that cyber-espionage group attributed to Russia's Foreign Intelligence Service (SVR) has been using information exfiltrated from the company's corporate email environment.

The hackers are leveraging what they took in the November incident — which was **discovered in January** — to "gain, or attempt to gain, unauthorized access."

"This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised," Microsoft said.

Friday's warning concerns a cyber-espionage unit Microsoft calls Midnight Blizzard, which the U.S. government has linked to the SVR.

"It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549**

---

**FORM 8-K/A**

---

**CURRENT REPORT  
PURSUANT TO SECTION 13 OR 15(D)  
OF THE SECURITIES EXCHANGE ACT OF 1934**

**Date of Report (Date of earliest event reported) January 17, 2024**

---

**Microsoft Corporation**

---

**Washington  
(State or Other Jurisdiction  
of Incorporation)**

**001-37845  
(Commission  
File Number)**

**91-1144442  
(IRS Employer  
Identification No.)**

**One Microsoft Way, Redmond, Washington**

**98052-6399**

<https://www.sec.gov/Archives/edgar/data/789019/000119312524062997/d808756d8ka.htm>

---

As disclosed in the Original Filing, the Company detected that beginning in late November 2023, a nation-state threat actor had gained access to and exfiltrated information from a very small percentage of employee email accounts including members of our senior leadership team and employees in our cybersecurity, legal, and other functions. Since the date of the Original Filing, the Company has determined that the threat actor used and continues to use information it obtained to gain, or attempt to gain, unauthorized access to some of the Company's source code repositories and internal systems. The threat actor's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. Our active investigations of the threat actor's activities are ongoing, findings of our investigations will continue to evolve, and further unauthorized access may occur.



“We have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We continue to coordinate with federal law enforcement with respect to its ongoing investigation of the threat actor and the incident.”

“As of the date of this filing, the incident has not had a material impact on the Company’s operations. The Company has not yet determined that the incident is reasonably likely to materially impact the Company’s financial condition or results of operations.”

# STORM ⚡ WATCH

CYBERSECURITY NEWS

# TOOL TIME







referefref / aiocrioc



<> Code

Issues

Pull requests 1

Actions

Projects

Security

Insights



main

aiocrioc / README.md

Go to file

t



referefref Bug in install logic



5402ccb · last month

History

186 lines (182 loc) · 5.92 KB

Preview

Code

Blame

Raw



# aiocrioc

<https://github.com/referefref/aiocrioc>

An LLM and OCR based Indicator of Compromise Extraction Tool. Built as a POC to compare against straight regex and OCR see: [ioc-ocr-extractor](#) The LLM version does significantly better at understanding the context of indicators like domains and file extensions which are often confused with plain regex (such as .com)

## Setup (tested on Ubuntu 22.04 with python3-venv)

```
# Download and install requirements  
apt install tesseract-ocr python3 python3-venv git -y
```





<https://www.riskmap.com/>

Search by IP, Port, CVE, Date etc.

### Cyber Threat Intelligence Indicator Search

This website employs a local json based search function to reduce the attack surface and keep this website static, please be patient while the search.json loads, this may take up to 30 seconds before the function becomes available.

### Cyber Threat Intelligence

- [Threat Feed Endpoint - Updated Daily](#)
- [Daily STIX2 Reports - Updated Every Day](#)
- [STIX2 Validator](#) - An online STIX2 JSON validator
- [Anonymous Proxies - Daily List](#)
- [Forum Spam - Daily List](#)
- [Phishing Domains - Daily List](#)
- [PulseDive Feed](#)
- [Alienvault OTX Feed](#)
- [MISP Default Feed](#)
- [All CTI](#)

### Deception Tech

- [modpot](#) - A modular web-application honeypot platform built with Golang and Gin
- [Honeydet](#) - A universal honeypot detector written in Go!
- [honeypage](#) - A golang tool for flattening HTML, CSS, JS into a single file for use with modpot
- [AICRIOC](#) - An LLM and OCR based Indicator of Compromise extraction and context tool built with Python and compatible with openAI compatible API endpoints
- [IOCOCRExtractor](#) - A pure regex and OCR (tesseract) Indicator of Compromise extractor tool built in Python for comparison to LLM extractions (see above)
- [SMTPLLPot](#) - An SMTP honeypot that uses OpenAI compatible APIs
- [Canary Token Detector](#) - A Think Canarytoken detector and nullifier tool
- [HoneyFS \(LLM Honeypot Filesystem Creator\)](#) - A tool for generating realistic and random filesystems using GPT3.5
- [Honeypot-ftp-python3](#) - A fork of Alex Bredo's FTP honeypot with python3 support and added features
- [AMTHoneypot-ng](#) - A fork of Haxrob's AMT Firmware Vulnerability (CVE-2017-5689) honeypot with added features
- [DSHP-ng](#) - A fork of Damn Simple HoneyPot rebuilt for python3 with verbose output
- [honeyprint-ng](#) - A fork of Glaslos' printer honeypot - migrated to python3 with added features. Includes a port of pkipplib to python3

### Other Projects

- [gitdoorcheck](#) - A git repo static code analyser using OpenAI LLMs written in Python
- [Vulnonym.org](#) - An (offensive) unique name generator for vulnerabilities, in contrast to Carnegie Mellon and NIST's approach
- [HACK THE UNIVERSE](#) - A book on the topic of the simulated universe, information theory, and consciousness
- [Toddler Recipes Australia](#) - A long running generative website that writes recipes complete with recipe schema markup

### General



# STORM ⚡ WATCH

CYBERSECURITY NEWS

# JUST FOR FUNSIES







ICS/OT SECURITY

INSIDER THREATS

## 'The Weirdest Trend in Cybersecurity': Nation-States Returning to USBs

USBs are fetch again, as major APTs from Russia, China, and beyond are turning to them for BYOD cyberattacks.

<https://www.darkreading.com/ics-ot-security/weirdest-trend-cybersecurity-nation-states-usb>



March 7, 2024





# Users Really Do Plug in USB Drives They Find

Matthew Tischer<sup>†</sup> Zakir Durumeric<sup>‡†</sup> Sam Foster<sup>†</sup> Sunny Duan<sup>†</sup>  
 Alec Mori<sup>†</sup> Elie Bursztein<sup>◇</sup> Michael Bailey<sup>†</sup>

<sup>†</sup> University of Illinois, Urbana-Champaign   <sup>‡</sup> University of Michigan   <sup>◇</sup> Google, Inc.  
 {tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu  
 zakir@umich.edu   elieb@google.com

**Abstract**—We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive’s appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.

## I. INTRODUCTION

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, whether driven by altruistic motives or human curiosity, the user unknowingly opens their organization to an internal attack when they connect the drive—a physical Trojan horse. Our community is filled with anecdotes of these attacks and pentesters have even boasted that they can *hack humans* by crafting labels that will pique an individual’s curiosity [19]: “While in the bathroom, I place an envelope in one stall. On the cover of the envelope I put a sticker that says PRIVATE. Inside the ‘private’ envelope is a USB key with a malicious payload on it. I do this in one stall and also in the hallway by a break room to increase my chances and hope that the person that finds one of them is curious enough to insert it into their computer. Sure enough, this method seems to always work.”

However, despite recent attacks that underscore the risk of malicious peripherals [39], [55] and rumors of the attack’s efficacy, there has been little formal analysis of whether the attack is effective nor why users connect the drives. In this work, we investigate the classic anecdote by conducting a large scale experiment in which we drop nearly 300 flash drives of different types, in different locations, and at different times on the University of Illinois, Urbana-Champaign campus.

We measure the efficacy and speed of the attack by replacing expected files on the drive with HTML files containing an embedded `img` tag that allows us to track when a file is opened on each drive without automatically executing any code. We find that users pick up and connect an estimated 45%–98% of the drives we dropped. Further, the attack is expeditious with a

median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner—suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files—such as vacation photos—before trying to find the drive’s owner.

To better understand users’ motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the precautions they took, demographic information, as well as standard questions to measure their risk profile and computer expertise. We find that attack was effective against all sub-populations at Illinois. The majority of respondents connected a drive to locate its owner (68%) or out of curiosity (18%), although a handful also admitted they planned on keeping the drive for themselves.

The students and staff that connected the drives were not computer nor security illiterate and were not significantly different than their peers at the University of Illinois on Egelman and Peer’s Security Behavior Intentions Scale (SeBIS) [12]. While the users that connected the drive engaged in riskier behavior than their peers on the DOSPERT scale [4], they were more risk averse than the general population in every domain except for recreational risk.

When prompted, 68% of users stated that they took no precautions when connecting the drive. For those respondents who considered protective measures, 10 (16%) scanned the drive with their anti-virus software and 5 (8%) believed that their operating system or security software would protect them, e.g., “I trust my macbook to be a good defense against viruses”. Surprisingly, another 5 (8%) sacrificed a personal computer or used university resources to protect their personal equipment. In the end, all but a handful of the users who took precautions did so in an ineffective manner and the majority took no precautions at all.

These results—particularly the risk averseness relative to the general population on the DOSPERT scale—suggest that the attack would be effective against most users and that the average person does not understand the danger of connecting an unknown peripheral to their computer. We hope that by bringing these details to light, we remind the security community that

<https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45597.pdf>

# SHAMELESS SELF-PROMOTION





BLOGS

# ConnectWise ScreenConnect – CVE-2024-1709 & CVE-2024-1708

<https://censys.com/connectwise-screenconnect-cve-2024-1709-cve-2024-1708/>

SHARE



FEBRUARY 27, 2024

ABOUT THE AUTHOR



English









# STORM ⚡ WATCH

CYBERSECURITY NEWS

# TAG ROUND-UP





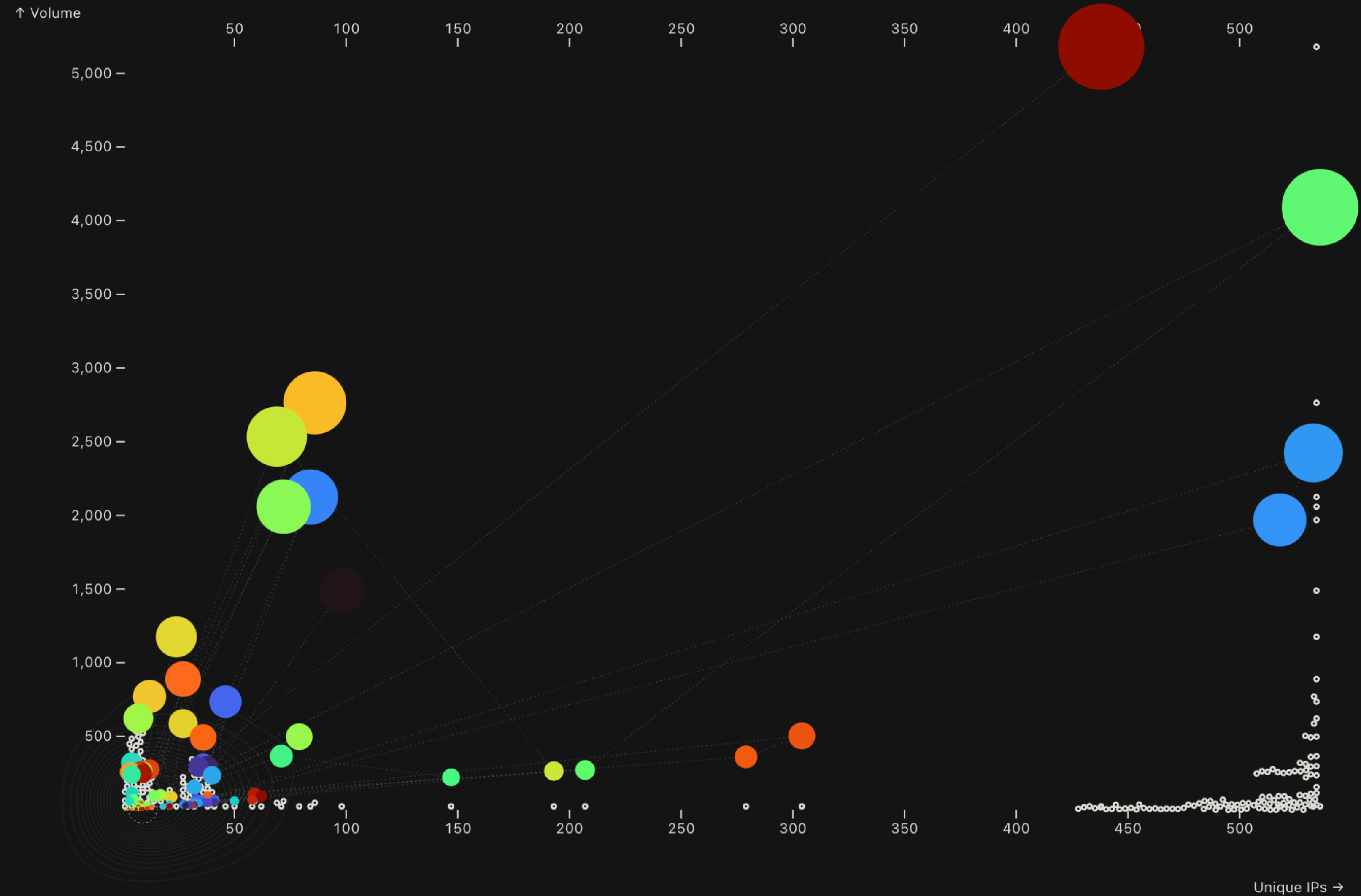
- WordPress KiviCare CVE-2022-0786 SQL Injection Attempt (CVE-2022-0786)
- Discuz Command Injection RCE Attempt
- ZhongYuan iAudit Command Injection RCE Attempt
- Nacos CVE-2021-29441 Backdoor Attempt (CVE-2021-29441)
- Nacos CVE-2021-29441 Vuln Check (CVE-2021-29441)

<https://viz.greynoise.io/trends?view=recent>

# IBM TN-3270 Mainframe Crawler

Unique IPs vs. Volume • Last seen activity: 2024-03-11

<https://viz.greynoise.io/tags/ibm-tn-3270-mainframe-scanner>



Yesterday is encircled; Side and bottom dots are marginal dot/distributions (similar to histograms). Lines connect dots as if in a time series plot. Dot size is proportional to the volume.



**WE NEED  
TO TALK  
ABOUT  
KEY**





# It Has Been 5 Days Since The Last KEV Release

<https://kev.hrbrmstr.app>



**CVE-2023-21237:** Android Pixel Information Disclosure

**CVE-2021-36380:** Sunhillo SureLine OS Command Injection

**CVE-2024-23225:** Apple iOS and iPadOS Memory Corruption

**CVE-2024-23296:** Apple iOS and iPadOS Memory Corruption

**CVE-2024-27198:** JetBrains TeamCity Authentication Bypass

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>