GREYNOISE

DECODING 2023

A GREYNOISE RETROSPECTIVE ON INTERNET EXPLOITATION

Preface

On behalf of the entire GreyNoise team, I'm excited to share our second annual Mass Exploitation Report. In this report, we'll cover some high-level findings and patterns we've observed over the past calendar year, as well as some details around how we observed them and what they might mean in the future.

As a brief reminder, GreyNoise operates a massive network of fake computers and services that lure attackers into revealing their tactics to us; then we share the technical details of those tactics with the cybersecurity community so that we can all learn from them and better defend ourselves, ultimately to make the internet a safer place. Our network of fake computers and services is massive and intelligent—it's easy to grow and can adapt quickly as needed.

In 2023, we watched the security community (both government and private sector) increasingly institutionalize our observations; our fellow security vendor partners are integrating more of our data than ever; and, government agencies (and news media) cite our observations regularly, which is great! The other side of this coin is that, for the first time in 2023, we directly observed attackers change their behaviors to avoid our detection capabilities.

The time between software vulnerabilities becoming public and attackers using them at large scale continues to decrease. But the approach we use to respond continues to be effective. And so, at GreyNoise, we will continue to make our detection network larger and smarter, and share the attacker behaviors we observe with the world as quickly as possible.

Ulysses S. Grant said that the art of war is simple—you must find where the enemy is and strike them as hard as possible as quickly as possible. My opinion is that, despite all the technical and market complexities, the art of defense is simple as well: you must find the attacks the enemy is using, report where they are coming from, and render them useless as quickly as humanly possible. I believe this report is a proof point at our progress in doing just this.

Thank you for continuing to trust myself and my colleagues at GreyNoise, and thank you for taking the time to read this report. I hope you will find its contents useful in the Sisyphean fight to make the internet a bit safer for everyone.

Onward,

Andrew Morris
Founder, CEO
GreyNoise Intelligence, Inc.

Contents

Introduction

Mass Exploitation

mass ex·ploi·ta·tion
|ˈmas ˌek-ˌsplȯi-ˈtā-shən|

The process where attackers systematically exploit a specific vulnerability across a large number of systems or networks. This is typically done using automated tools or scripts, and the aim is to either affect as many victims as possible in the shortest amount of time, or compromise a targeted list of organizations. Common scenarios include the use of a zero-day, or "n"-day vulnerability, where the exploit code is used widely before research teams and incident response teams can mitigate it, usually after a public proof-of-concept (PoC) is announced.

The internet, as a whole, is never silent.

Yes, a region may suffer a catastrophic natural disaster, or a regime could deem it necessary to "pull the plug" for a short period of time. But, there will always be some baseline level of noise that often resonates far and wide across the internet. Within this noise there are certain malicious tones which are reverberating at frequencies designed to shatter the glass-like defenses of specific components in IT infrastructure.

The GreyNoise platform, powered by the skills and expertise of our research, design, and engineering teams, is crafted to identify these cyber-acoustic events and help organizations cancel out harsh frequencies before they do real, measurable harm.

If you had been using GreyNoise in 2023 what dissonant chords would you have known about in advance and been able to mute? This is the question our annual Mass Exploitation Reports help you answer.

Why is this important?

There are two main reasons.

First, at the heart of the issue lies a significant dichotomy: many threat intelligence providers excel in identifying potential indicators of compromise. However, due to 2nd or 3rd party collection methods and the industry pressure to never miss anything bad, this catch-all approach has resulted in lower quality data. What's more, and most importantly, this data is not tailored to the consumer nor actionable within their environment. A notable number of these products also exhibit a reluctance to offer decisive recommendations for implementing automated blocking decisions derived from their data. This raises a pertinent question: if machines cannot effectively and immediately make automated decisions based on source data, can their utility be genuinely considered effective?

Second, internet architecture is becoming increasingly more complex and a bear to manage. This makes every organization with an internet presence prime targets for attackers specializing in gaining initial access or launching denial of service (DoS) attacks. And, as we'll see in the section on "Nation State Conflicts And Their Very Real Impact On Mass Exploitation," the evolution of nation state conflicts is also putting virtually every organization in the crossfire.

The GreyNoise platform, including our vast sensor network, is designed to identify these probes and attacks with pinpoint precision at the very moment they occur. No matter where adversaries aim their attacks, GreyNoise is there. No matter how many packets they sling, our systems analyze them instantly, enabling us to identify and communicate even the oddest trends and anomalies. This gives defenders the tools and data they need to stop attacks before they start, plus buy time to focus on patching, mitigation, and response.

This report presents multiple segments detailing various key aspects of major mass exploitations of 2023. We encourage you to view the year through the perspective of a defender, say on a security operations (SOC) team, with limitless access to GreyNoise data. From this vantage point, see how 2023 might have appeared if you had utilized our datasets* to remain at the forefront of thwarting widespread internet exploits.

** There is of course no silver bullet - but we as a company are aiming to make your sometimes impossible (but always imperative) job a bit easier.*

EXECUTIVE SUMMARY

2023 GreyNoise By The Numbers

GreyNoise Tags

In 2023, GreyNoise produced **290 new tags/detections covering 242 Common Vulnerabilities and Exposures (CVEs)** to help organizations proactively identify and respond to internet probes and attacks

Sixty-seven (67) of these tags created in 2023 have corresponding entries in CISA's Known Exploited Vulnerabilities (KEV) catalog, 34% (23) of which are also known to be associated with ransomware attacks.

We'll go deeper into the KEV view in a forthcoming section.

2023
290 Tags
242 CVEs
67 CISA KEV References

Total
1,126 Tags
705 CVEs
259 CISA KEV References

GreyNoise Platform

Across 2023, over 17.3 million valid GreyNoise GNQL queries were submitted by humans or integrations. These came from over 195 geolocated source countries.

The top five tags explored include:

- Citrix Adc NetScaler Information Disclosure Attempt (CVE-2023-4966)
- Huawei HG532 UPnP Worm (CVE-2017-17215)
- RealTek Miniigd UPnP Worm (CVE-2014-8361)
- GPON Router Worm (CVE-2018-10561)
- Netgear Command Injection (CVE-2016-6277)

And, according to what folks were searching for, 5.188.210.227 appears to be the naughtiest IP address.

GreyNoise Sift

Our AI-enabled Sift threat-hunting platform gives our detection engineers bionic powers when it comes to identifying novel or just "recently first seen" HTTP payloads. While we've been tweaking the underlying models since the start of 2023, Sift has "officially" been online since September and has processed nearly 300 million HTTP payloads from our sensor fleet.

From that corpus, Sift discovered over 8.1K unique new traffic clusters of 1.17+ million HTTP payloads. These have resulted in over two dozen new tags, with scores more in the backlog and ready to be incorporated into the platform in the coming weeks.

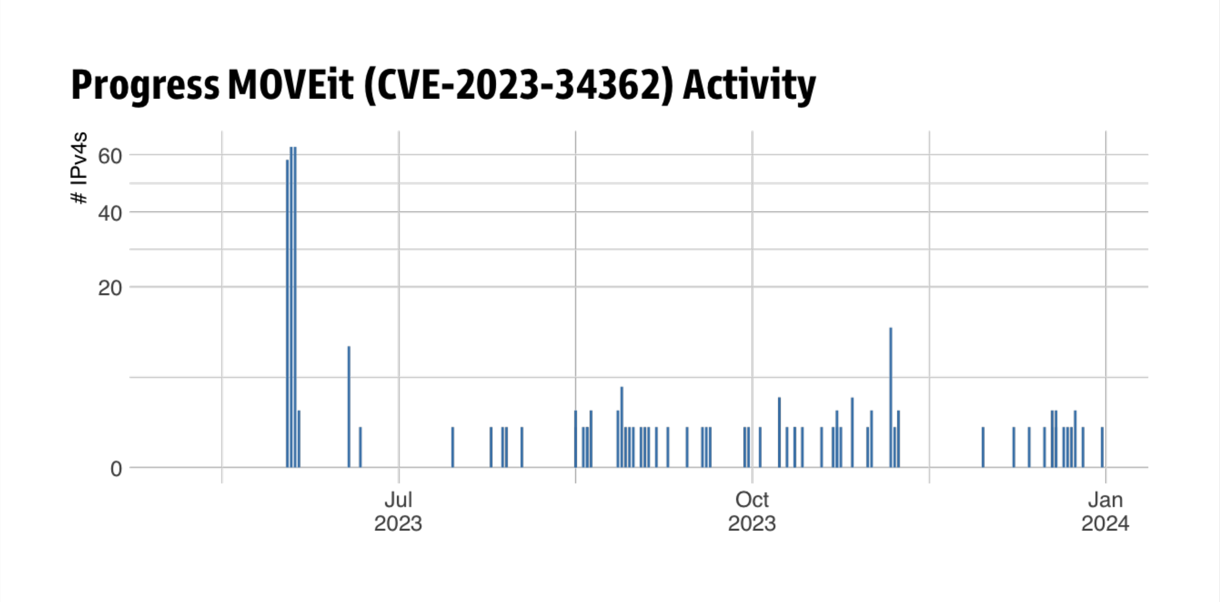
We plan on extending Sift's capabilities beyond HTTP in 2024, enabling novel cluster detections at scale for arbitrary payloads.

Critical Exploits Of 2023

Not all CVEs, or exploits, are created equal. Some definitely stood out — in an overall impactful way — from the 242 found in our 2023 tag corpus. Here's a short list of three of the most critical exploits of 2023.

Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362)

MOVEIT TRANSFER SCANNER | GREYNOISE VISUALIZER



CVE-2023-34362 was publicly disclosed on May 31, 2023, by Progress Software. However, it had been exploited in the wild for several weeks before disclosure. The Cl0p ransomware group was one of the first attackers to exploit this vulnerability, using it to steal data from many high-profile organizations.

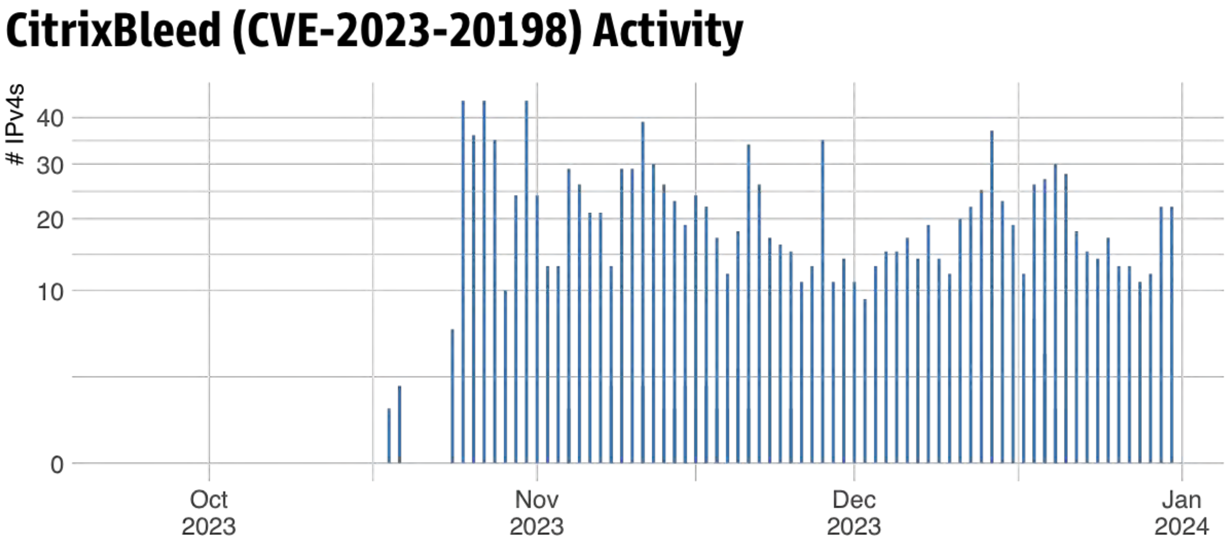
According to KonBriefing Research, we ended the year with a victim tally of over 2.6K organizations and ~90 million individuals. The most affected sectors include education, healthcare, and financial and professional services. Some organizations that reported significant data breaches include the Colorado Department of Health Care Policy and Financing and the State of Maine. This tracks with other data sources, such as regular ransomware reports by Emsisoft, which notes that state and local governments and municipalities are, increasingly, successfully targeted by ransomware actors. This is unsurprising, given how difficult it is to acquire funding levels necessary to staff and empower these agencies.

GreyNoise continued to see activity on this tag throughout the remainder of 2023 and expect this exploit to become part of the regular drumbeat of background internet noise for years to come.

More information: CVE-2023-34362

Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability (CVE-2023-4966; a.k.a., CitrixBleed)

CITRIX ADC NETSCALER INFORMATION DISCLOSURE ATTEMPT



CitrixBleed, officially known as CVE-2023-4966, is a critical vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway appliances. It allows threat actors to hijack authenticated sessions from these devices, bypassing multifactor authentication and password requirements.

Multiple hacker groups, including LockBit ransomware, have actively exploited this vulnerability, with some groups even automating the attack process. One of the most prolific breaches caused by CitrixBleed was suffered by Comcast.

GreyNoise continues to see daily mass exploitation attempts from an average of 30 unique IPv4 addresses per day.

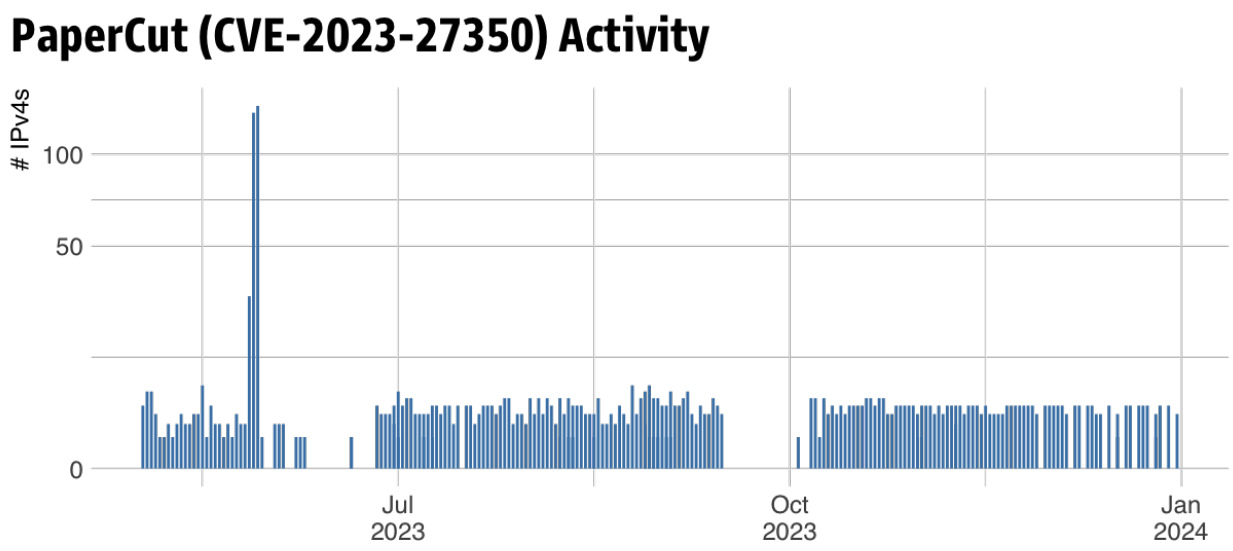
More information: CVE-2023-4966

Next page: PaperCut MF/NG Improper Access Control Vulnerability

PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350)

PAPERCUT RCE ATTEMPT

PAPERCUT AUTHENTICATION BYPASS CHECK



Based on data from the FBI, cybercriminals began exploiting the vulnerability identified as CVE-2023-27350 from mid-April 2023 and have continued to do so until now. In a separate revelation from the FBI in early May 2023, it was reported that a collective known as the Bl00dy Ransomware Gang attempted to target vulnerable PaperCut servers, particularly within the Education Facilities Subsector.

GreyNoise continues to see weekly check and exploit attempts, showing this PaperCut is not going to heal any time soon.

- More information: CVE-2023-27350

We covered some of these and more in our 2023 year-end tag roundup blog series, and you can always peruse our entire tag catalog to see if technologies you use are actively targeted by various adversaries.

One lesson to learn from these and other exploits of 2023 is that attackers know the critical weak spots in organizations — remote access and file-sharing technologies — and are relentless in their pursuits to exploit them. While organizations can use GreyNoise detections to help mitigate known threats, defenders should also focus on shoring up these components' configurations, enhancing telemetry from hosted systems, and keeping a watchful eye on anomalous behavior and vendor patch announcements.

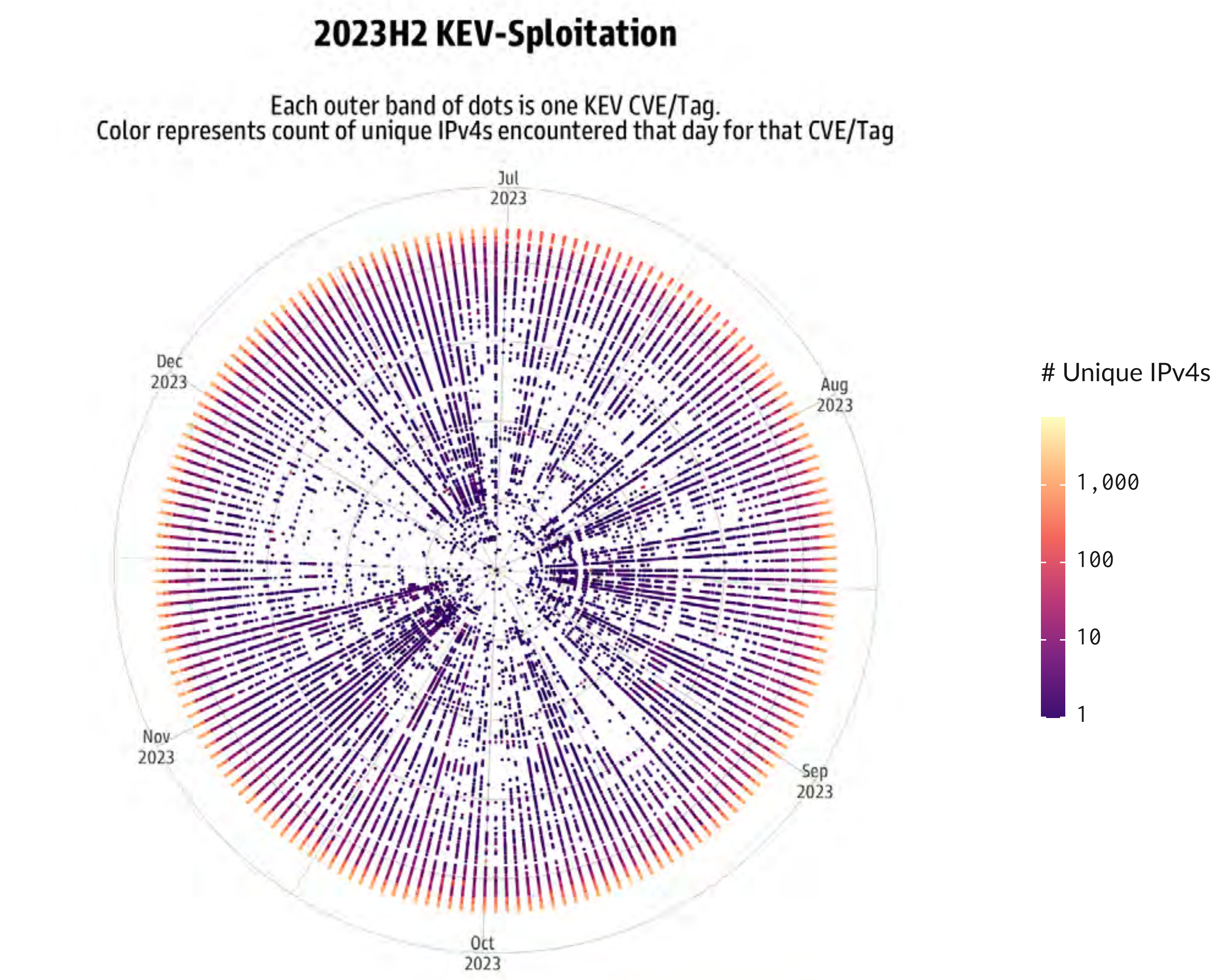
GreyNoise Tags: The CISA KEV Perspective

It is no secret that GreyNoise researchers are huge fans of CISA's Known Exploited Vulnerabilities (KEV) catalog. Their criteria for list inclusion:

- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor-provided update.

Combined with their independent analyses and broad information-sharing network, KEV helps CISA avoid the perils of the hype cycle and gives defenders within and outside the U.S. government a tangible, focused list of active threats they should absolutely take time to remediate/patch now.

Not all CISA KEV CVEs can be observed in the GreyNoise sensor fleet. Our researchers focus on exploits that can be observed over the internet, and ones that are exploitable without credentials (or, at least, without default credentials). As noted above, this means that there are 67 corresponding GreyNoise "KEV" tags in 2023, making a grand total of 259. The following visualization provides some "feel" for what that activity looks like across GreyNoise:



We’re also a bit proud of our track record regarding coverage for “GreyNoise-able” KEV CVEs. We meet or beat CISA nearly 63% of the time when it comes to having a published tag for a CVE that enters their catalog. This makes it much easier for federal agencies to meet or exceed remediation time requirements. It’s also helpful in the same way if your organization is tracking with KEV.

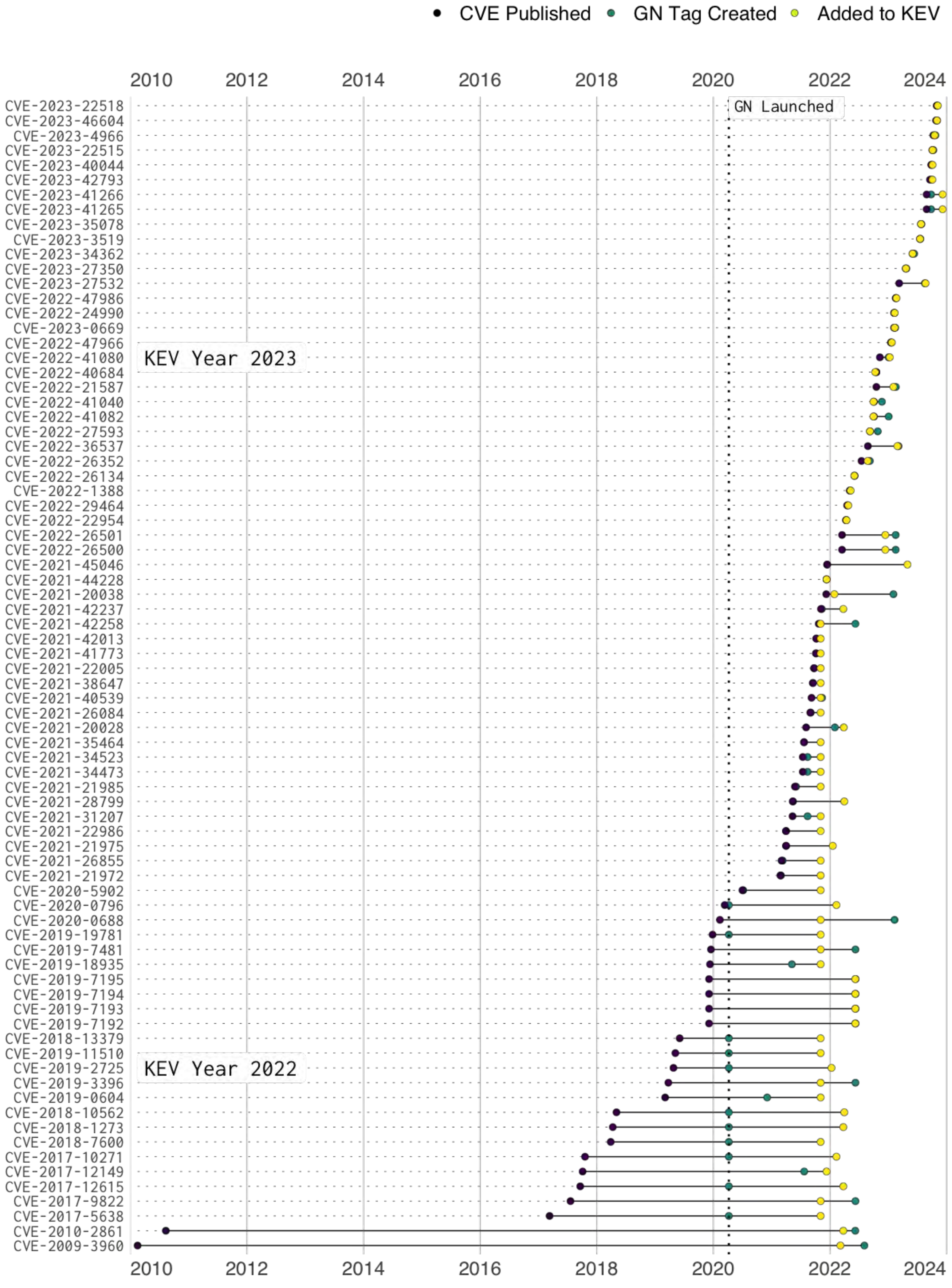
In the latter half of 2023, CISA added a field to help defenders know if a particular exploit was used by ransomware actors. Given how devastating these attacks can be, this tiny bit of extra metadata can help agencies and organizations further prioritize and gain internal traction for remediation efforts.

214 (20%) of all CISA KEV CVEs are known to be used in ransomware attacks, and 34 (18%). GreyNoise has tags for 78 of all these CVEs — virtually all of which are associated with a means of gaining initial access to vulnerable infrastructure.

As the chart below shows, both CISA and GreyNoise are closing the gap between CVE coverage and the start of exploitation campaigns. This is great news for both defenders and those at risk of identity or information exposure.

CISA/GreyNoise Ransomware CVE Coverage Delta

While some older initial access CVEs had ample time to be exploited unawares, more recent ones are almost immediately found in both KEV and GreyNoise, giving defenders more of a fighting chance.



We look forward to increased collaboration in 2024 with one of the U.S. Government's most successful public-private partnerships.

//

Nation State Conflicts And Their Very Real Impact On Mass Exploitation

We cannot let 2023 go into the record books without some mention of the part that nation state conflicts have had on the mass exploitation landscape.

The present major conflicts between Russia/Ukraine, Israel/Hamas, and other regional hostilities play out in both kinetic/physical (guns/bombs) and cyber fields of battle, and the impacts of those operations are not always contained to just the engaged parties.

Unlike kinetic battles, where ordinance generally has some limited range, battles in cyberspace can have spillover effects that put noncombatants at equal or greater risk. It's also possible to get caught up in the middle of these operations just by using technologies aligned to one or more of the combatants. The most recent example of this is from a report by the Security Service of Ukraine. In it, they report the takedown of two residential surveillance cameras that were hacked by Russia and abused to spy on air defense systems and critical infrastructure in Kyiv. They further note they have "blocked the operation of 10,000 IP cameras that the enemy could have used to adjust missile attacks on Ukraine".

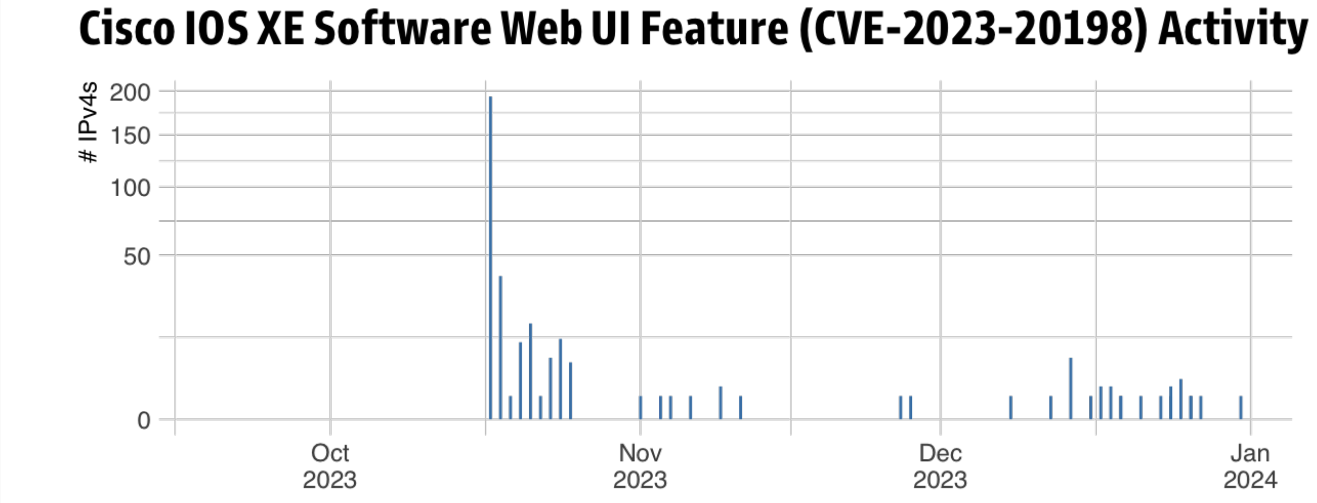
Let's make this discussion even more tangible through the lens of two recent 2023 vulnerabilities in other internet-facing components.

CVE-2023-20198 Cisco IOS XE Web UI Privilege Escalation Vulnerability

In October, Cisco released an advisory for "Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature" (CVE-2023-20198). Matthew Remacle from GreyNoise Lab did a deep dive into this vulnerability soon after the advisory was released. GreyNoise had tag coverage for it on October 20, 2023, and CISA added CVE-2023-20198 to KEV on October 23, 2023.

In November, CISA added an Industrial Control Systems (ICS) Advisory for Rockwell Automation Stratix 5800 and Stratix 5200 systems, which also run embedded Cisco IOS XE Software.

As noted in said blog post, and these advisories, this vulnerability was, and is still,



Source: <https://viz.greynoise.io/tag/cisco-ios-xe-privilege-escalation-attempt?days=30>

especially disconcerting. These devices generally have fixed IP addresses, and the exploit afforded deep, privileged access to these critical systems and the networks behind them. Thousands of them were repeatedly compromised, and GreyNoise has observed a number of these known, fixed IP addresses being used in both probes and attacks that are clearly aimed at infrastructure in both Israel and Ukraine. We also still see daily [re]compromising attempts.

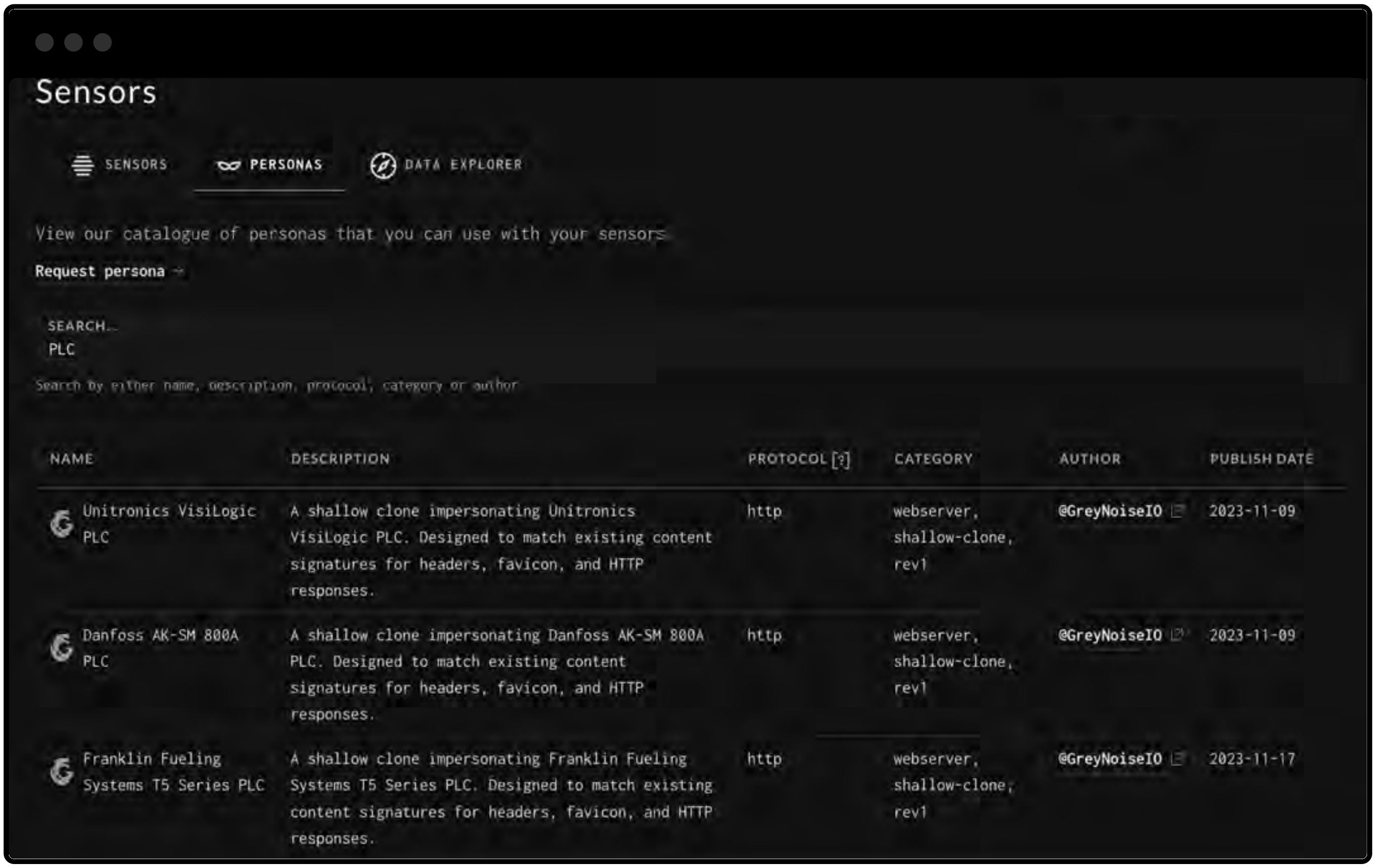
We have no direct evidence that attacker groups launched the broad Cisco IOS XE exploit campaign as a cover for these direct operations. However, this situation shows how unpatched internet-facing infrastructure can be co-opted to be used in conflict zones.

CVE-2023-6448: Unitronics Vision PLC and HMI Insecure Default Password Vulnerability

In terms of direct spillover effects, CISA issued a warning about attacks on a specific tool used by water and wastewater systems — yet another area where staffing and funding levels are challenging to improve — the Unitronics PLC, which is a product from Israel. The advisory was linked to a notice from the Water Information Sharing and Analysis Center (WaterISAC) and the American Water Works Association (AWWA). The hackers claimed to be attacking water and energy facilities using products from Israel.

There was a confirmed attack on the Municipal Water Authority of Aliquippa (Pennsylvania) involving an exploit for this PLC vulnerability.

GreyNoise Labs has a series of PLC sensors in our new sensor fleet, including this Unitronics PLC, where have and continue to see probes and exploitation attempts:



Sensors

View our catalogue of personas that you can use with your sensors

Request persona →

SEARCH... PLC

Search by either name, description, protocol, category or author

NAME	DESCRIPTION	PROTOCOL [?]	CATEGORY	AUTHOR	PUBLISH DATE
Unitronics VisiLogic PLC	A shallow clone impersonating Unitronics VisiLogic PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-09
Danfoss AK-SM 800A PLC	A shallow clone impersonating Danfoss AK-SM 800A PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-09
Franklin Fueling Systems T5 Series PLC	A shallow clone impersonating Franklin Fueling Systems T5 Series PLC. Designed to match existing content signatures for headers, favicon, and HTTP responses.	http	webserver, shallow-clone, rev1	@GreyNoiseIO	2023-11-17

Our new sensors will be generally available to GreyNoise consumers in 2024 and will enable even more robust persona development and enhanced detections. This will further enable GreyNoise users to gain more advantage over attackers of every level of sophistication.

Country-Level Mass Exploitation

Meanwhile, if you're interested in what mass-exploitation looks like at the nation state level, you can peruse a snapshot of a sample of our country reports we produced in the latter half of 2023.

//

Active Defense And Incident Response With Tag Taxonomies

The telemetry from GreyNoise tags helps organizations quickly, proactively, and directly respond to emergent threats and pernicious exploits that never seem to go away. However, there's quite a bit more one can do with our data, especially the vulnerabilities covered in our malicious detections.

The vast majority of this malicious activity detected within the GreyNoise sensor fleet has associated CVEs. As a result, it's possible to further enrich this information with data from modern defender taxonomies such as MITRE ATT&CK, Common Attack Pattern Enumeration and Classification (CAPEC), and Common Weakness Enumeration (CWE).

Let's take a brief look at our tag corpus through those lenses.

CWE View Of GreyNoise Tags

As visualized in the above image, over 45 common weaknesses are represented across our tag corpus. Given the focus areas of GreyNoise, one will not be surprised that most of these center around ones that can be exploited remotely.

Seven CWEs make up over 70% of the entire tag corpus, and we're sad to report that it's 2024 and SQL Injection is still in the top ten of vulnerabilities when it comes to mass exploitation:

CWE	Weakness
CWE-78	OS Command Injection
CWE-22	Path Traversal
CWE-94	Code Injection
CWE-287	Improper Authentication
CWE-77	Command Injection
CWE-89	SQL Injection
CWE-502	Deserialization of Untrusted Data

When we perform the same commonality analysis against the MITRE ATT&CK framework, the following techniques are associated with 60% of the activity associated with CVEs in the GreyNoise corpus (See Appendix C for a full mapping of these ATT&CK Tactics to 2023 GreyNoise Tags):

Hijack Execution Flow (T1574)	This technique involves adversaries executing their own malicious payloads by manipulating how operating systems run programs. It can be used for persistence, privilege escalation, or evasion of defenses.
Access Token Manipulation (T1134)	Adversaries may modify access tokens to operate under a different user or system security context, which can be used to escalate privileges or bypass access controls.
Use Alternate Authentication Material (T1550)	This technique typically involves adversaries using different forms of authentication, such as passphrases, certificates, or Kerberos tickets, to access systems or data.
Abuse Elevation Control Mechanism (T1548)	This technique generally involves adversaries manipulating or bypassing mechanisms that control elevation or changes in privileges to gain higher-level permissions.
Server Software Component (T1505)	This technique is not detailed in the search results, but generally involves adversaries exploiting vulnerabilities in server software components to gain unauthorized access or control.
Remote Service Session Hijacking (T1563)	This technique is not detailed in the search results, but typically involves adversaries taking over a legitimate session between networked computers to gain unauthorized access.
Event Triggered Execution (T1546)	This technique is not detailed in the search results, but typically involves adversaries establishing persistence and executing malicious code by triggering certain events or conditions.

Similar mappings can be performed within CAPEC and other common frameworks.

Defenders can use this information to help inform active defense plans and improve telemetry captured from systems and devices to enable lightning-fast incident response, which may help prevent a truly catastrophic event.

While the “top” members of these taxonomy lists can and will change over time, here are some steps defenders can take in 2024 to help defend against these known impacts:

Monitor and control execution flow	Defenders should monitor for unusual process behavior that may indicate an attempt to hijack the execution flow. They should also control which programs can be executed to prevent adversaries from running malicious payloads.
Strengthen and monitor defenses	Defenders should ensure that their defensive measures, such as firewalls and anti-virus software, are robust and up-to-date. They should also monitor for changes that may indicate an attempt to impair these defenses.
Control and monitor access tokens	Defenders should control which processes can create or manipulate access tokens and monitor for unusual token activity that may indicate an attempt to escalate privileges or bypass access controls.
Patch vulnerabilities	Defenders should regularly patch and update their systems to fix known vulnerabilities that could be exploited by these techniques.

Conclusion

2023 saw numerous critical remote code execution and privilege escalation vulnerabilities disclosed in popular software, including Citrix, Atlassian Confluence, ownCloud, and Cisco networking devices to name a few. Time and time again, as soon as proof-of-concept exploits emerged, GreyNoise observed widespread scanning and exploitation attempts against vulnerable organizations.

Our threat intelligence platform successfully collected data on every IP address associated with opportunistic scanning threats for yet another year. We were and are quick to mobilize our detection engineering team to analyze exploit traffic, write custom network detection signatures, and apply descriptive metadata tags to each observed attacker. These tags were specific to the vulnerabilities and enabled security teams to quickly identify and block threats that targeted vulnerable systems.

While there is no single solution to the industry's numerous challenges, GreyNoise provides organizations with the information and telemetry necessary to understand what to prioritize to patch and to buy more time for patching. As the threat landscape continues to evolve in 2024, GreyNoise will remain vigilant—detecting emerging attacks based on real evidence, not fear, uncertainty, and doubt.

The integration of our new sensor network with cutting-edge AI and data science technologies is set to revolutionize the way defenders utilize our state-of-the-art threat intelligence. Deploying sensors where targeted attacks occur, and surfacing new attack patterns and clusters as they happen will provide unprecendeted views into what industries attackers are targeting, and what new techniques they are using. This combinaton will empower defenders to stay ahead of threats, focus on patching, mitigation, and response, and ultimately, make the internet a safer place.

Keep an eye on our blog, webcast/podcast, and platform for breaking news, exciting new capabilities, and information you can use to keep your organization safe from harm.

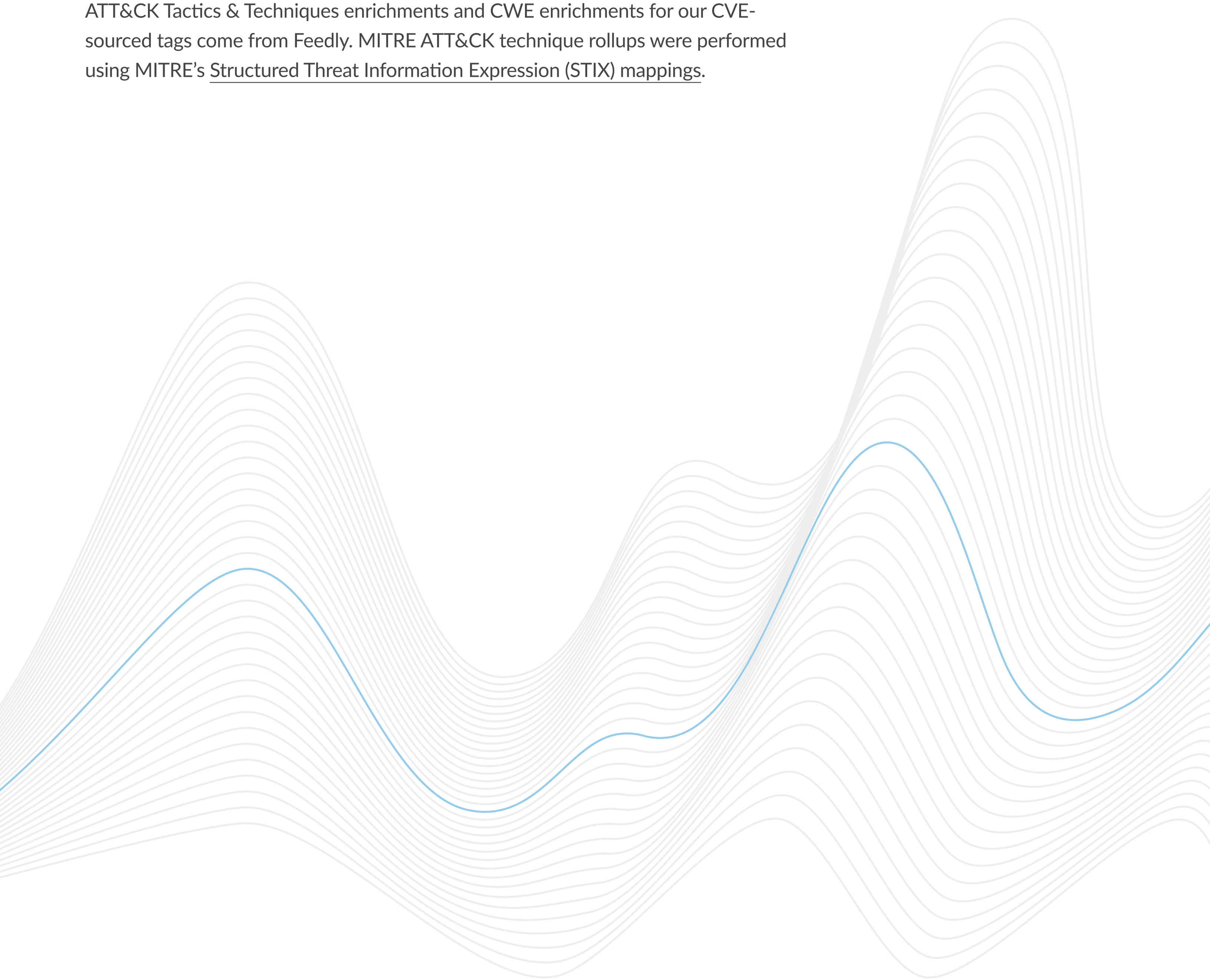
//

Appendix A: Methodology

All GreyNoise tag data comes from our tag corpus, with data collected by our planetary-scale sensor fleet. Geolocation enrichments are sourced directly from IPInfo.

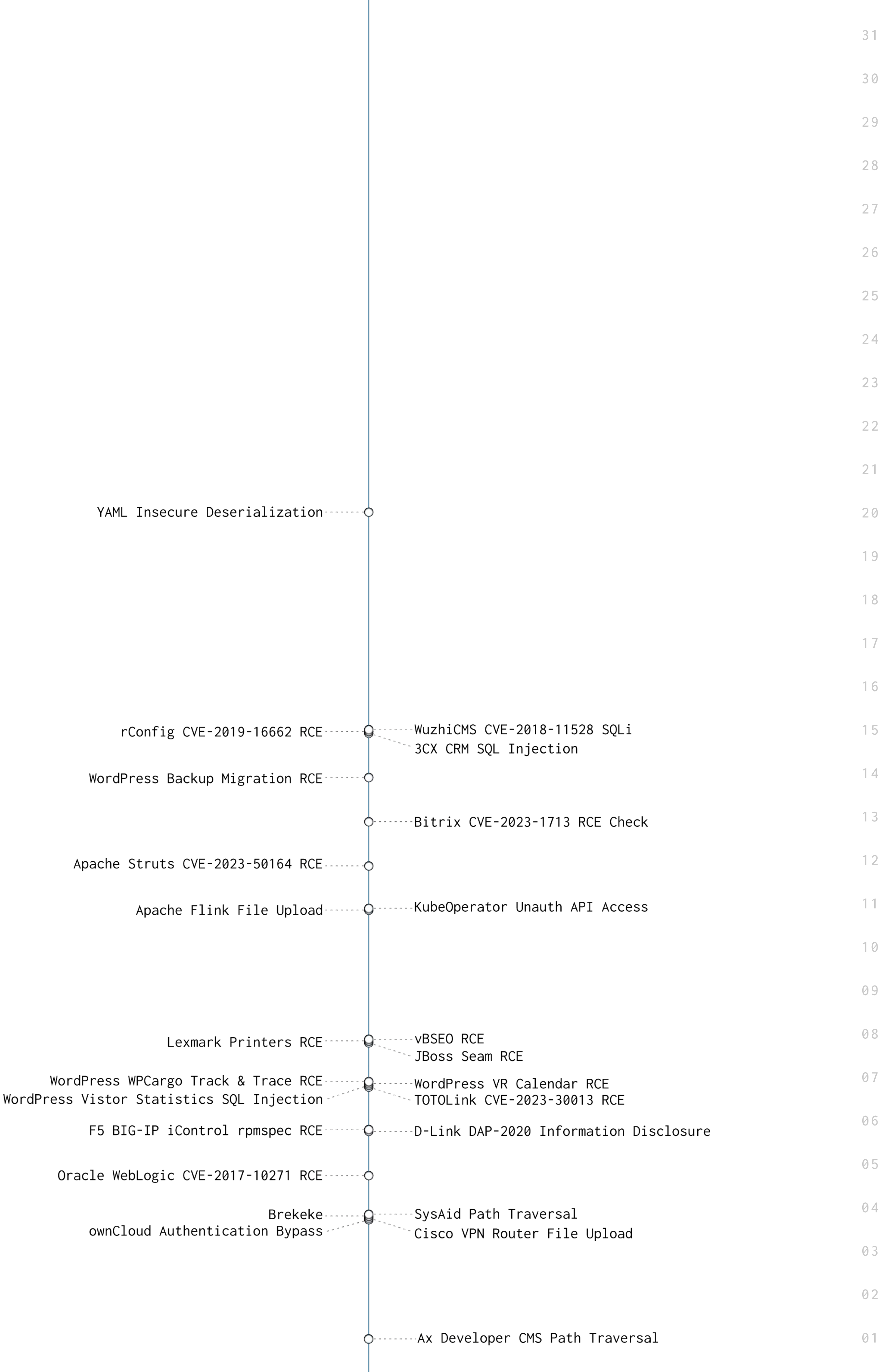
Data from CISA is sourced directly from their Known Exploited Vulnerabilities catalog.

ATT&CK Tactics & Techniques enrichments and CWE enrichments for our CVE-sourced tags come from Feedly. MITRE ATT&CK technique rollups were performed using MITRE's Structured Threat Information Expression (STIX) mappings.



December 2023

APPENDIX B: 2023 TAG TIMELINE



31
30
29
28
27
26
25
24
23
22
21

20 YAML Insecure Deserialization

19
18
17
16

15 rConfig CVE-2019-16662 RCE
WuzhiCMS CVE-2018-11528 SQLi
3CX CRM SQL Injection

14 WordPress Backup Migration RCE

13 Bitrix CVE-2023-1713 RCE Check

12 Apache Struts CVE-2023-50164 RCE

11 Apache Flink File Upload
KubeOperator Unauth API Access

10
09

08 Lexmark Printers RCE
vBSEO RCE
JBoss Seam RCE

07 WordPress WPCargo Track & Trace RCE
WordPress Vistor Statistics SQL Injection
WordPress VR Calendar RCE
TOTOLink CVE-2023-30013 RCE

06 F5 BIG-IP iControl rpmspec RCE
D-Link DAP-2020 Information Disclosure

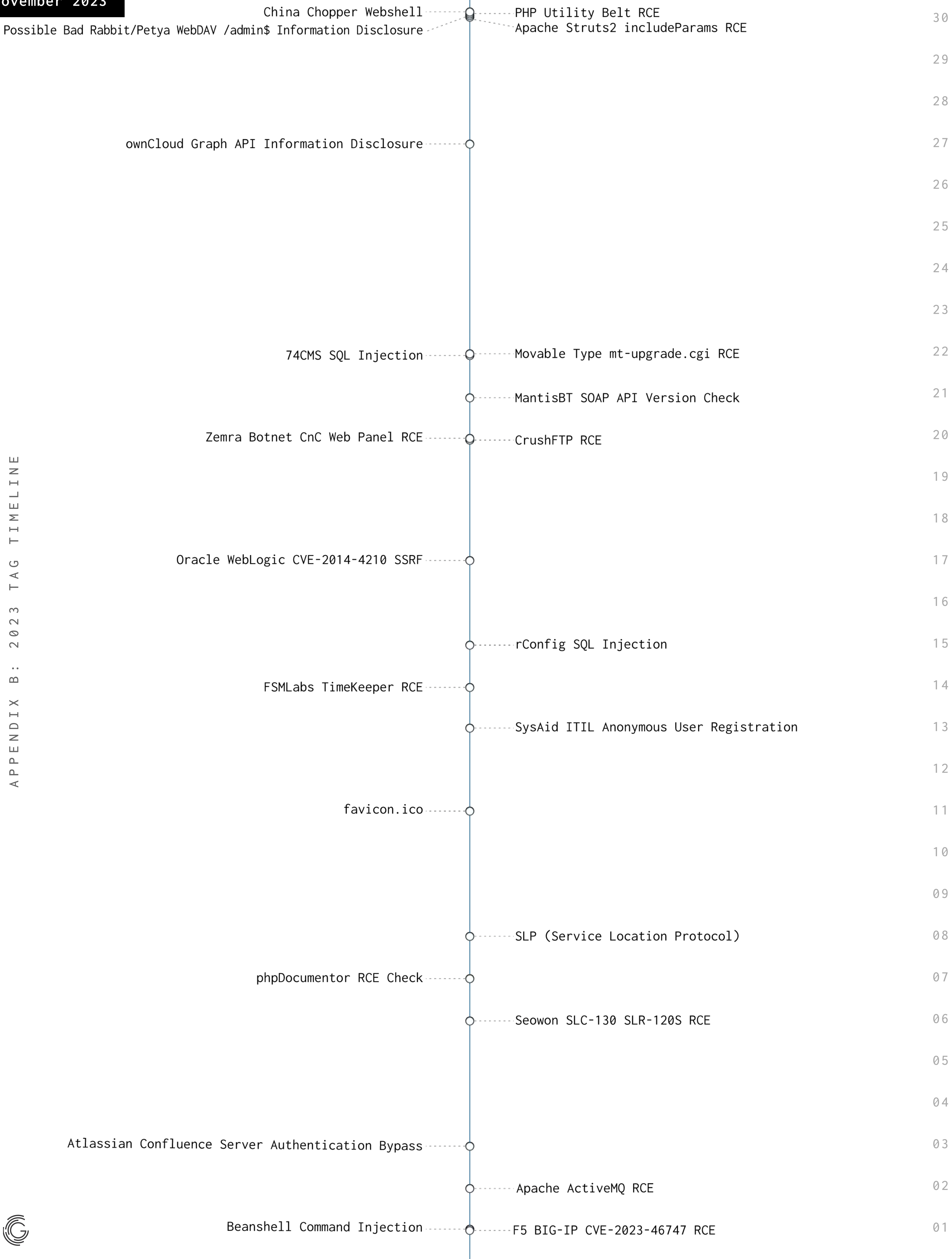
05 Oracle WebLogic CVE-2017-10271 RCE

04 Brekeke
ownCloud Authentication Bypass
SysAid Path Traversal
Cisco VPN Router File Upload

03
02

01 Ax Developer CMS Path Traversal

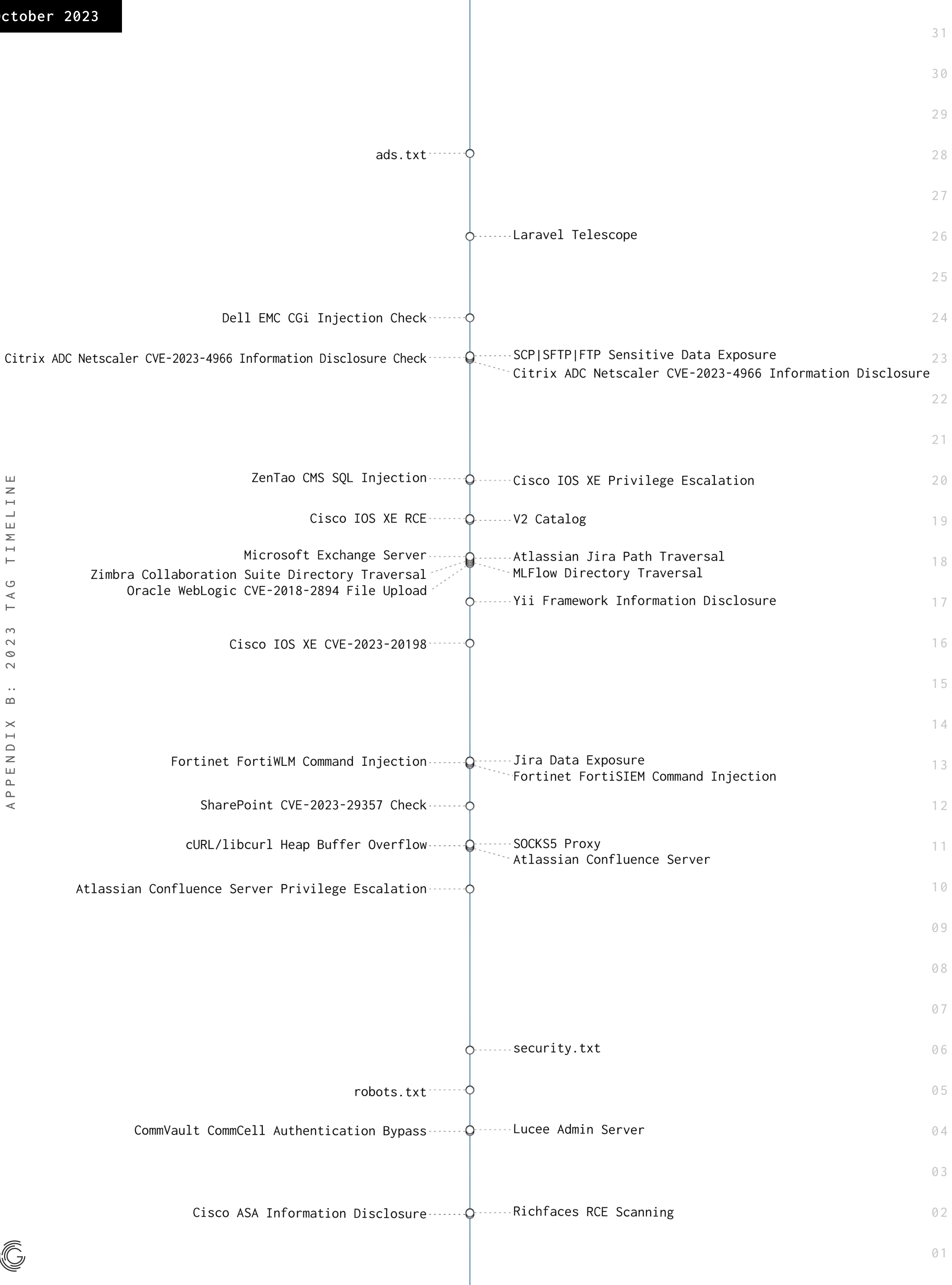
November 2023



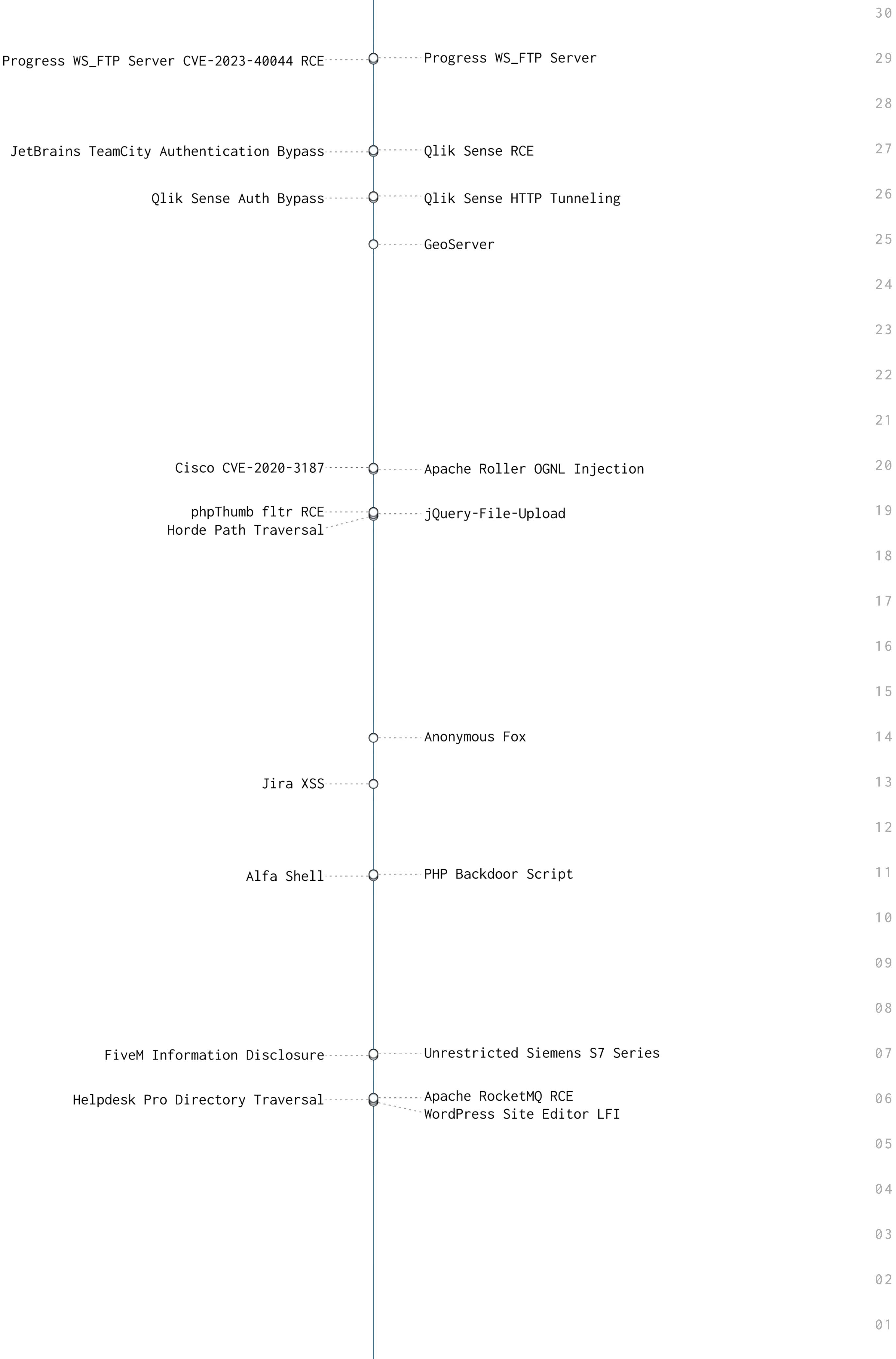
30	China Chopper Webshell Possible Bad Rabbit/Petya WebDAV /admin$ Information Disclosure	PHP Utility Belt RCE Apache Struts2 includeParams RCE
29		
28		
27	ownCloud Graph API Information Disclosure	
26		
25		
24		
23		
22	74CMS SQL Injection	Movable Type mt-upgrade.cgi RCE
21		MantisBT SOAP API Version Check
20	Zemra Botnet CnC Web Panel RCE	CrushFTP RCE
19		
18		
17	Oracle WebLogic CVE-2014-4210 SSRF	
16		
15		rConfig SQL Injection
14	FSMLabs TimeKeeper RCE	
13		SysAid ITIL Anonymous User Registration
12		
11	favicon.ico	
10		
09		
08		SLP (Service Location Protocol)
07	phpDocumentor RCE Check	
06		Seowon SLC-130 SLR-120S RCE
05		
04		
03	Atlassian Confluence Server Authentication Bypass	
02		Apache ActiveMQ RCE
01	Beanshell Command Injection	F5 BIG-IP CVE-2023-46747 RCE

October 2023

APPENDIX B: 2023 TAG TIMELINE



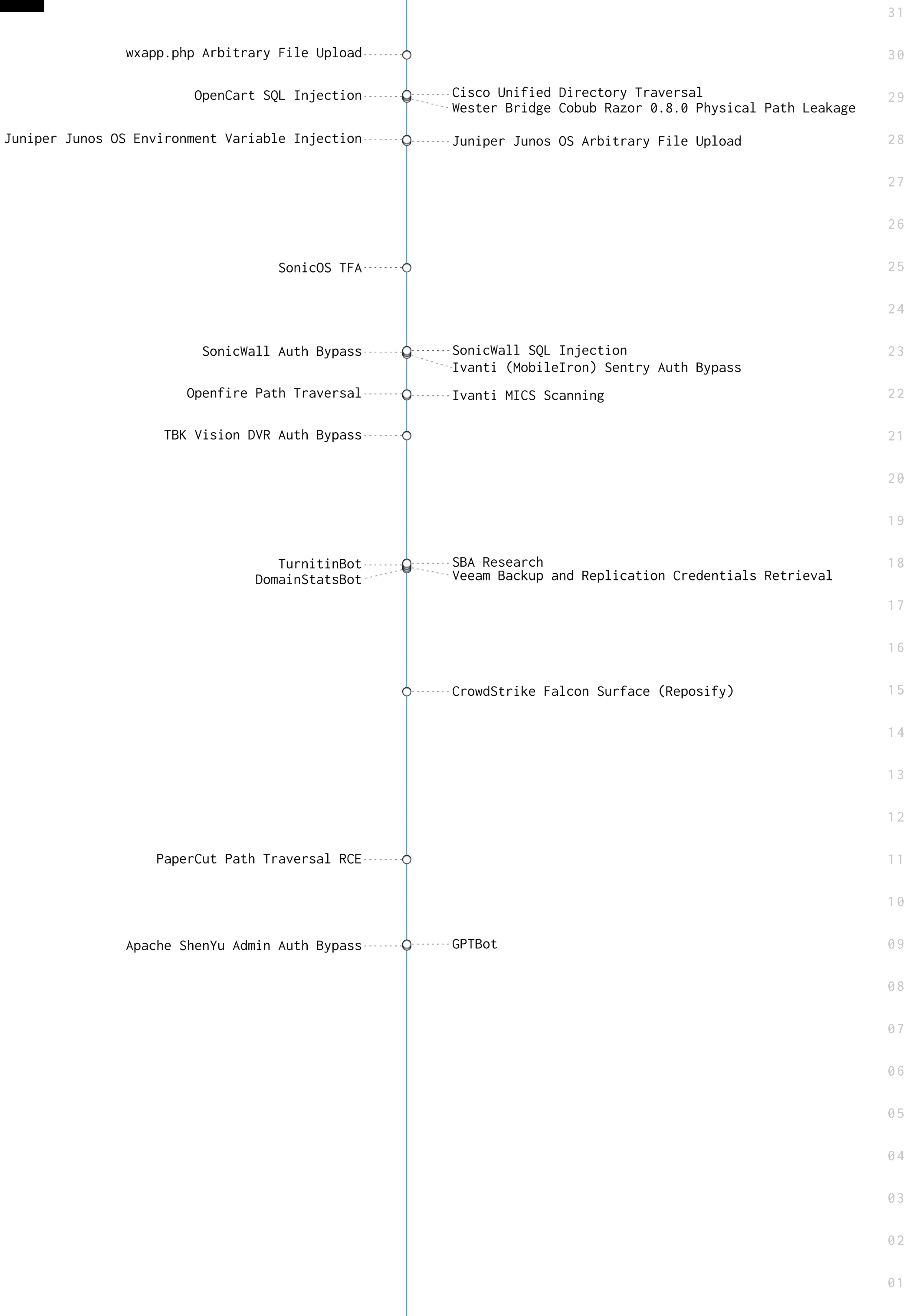
September 2023



30		
29	Progress WS_FTP Server CVE-2023-40044 RCE	Progress WS_FTP Server
28		
27	JetBrains TeamCity Authentication Bypass	Qlik Sense RCE
26	Qlik Sense Auth Bypass	Qlik Sense HTTP Tunneling
25		GeoServer
24		
23		
22		
21		
20	Cisco CVE-2020-3187	Apache Roller OGNL Injection
19	phpThumb fltr RCE Horde Path Traversal	jQuery-File-Upload
18		
17		
16		
15		
14		Anonymous Fox
13	Jira XSS	
12		
11	Alfa Shell	PHP Backdoor Script
10		
09		
08		
07	FiveM Information Disclosure	Unrestricted Siemens S7 Series
06	Helpdesk Pro Directory Traversal	Apache RocketMQ RCE WordPress Site Editor LFI
05		
04		
03		
02		
01		

August 2023

APPENDIX B: 2023 TAG TIMELINE



31

30 wxapp.php Arbitrary File Upload

29 OpenCart SQL Injection
Cisco Unified Directory Traversal
Wester Bridge Cobub Razor 0.8.0 Physical Path Leakage

28 Juniper Junos OS Environment Variable Injection
Juniper Junos OS Arbitrary File Upload

27

26

25 SonicOS TFA

24

23 SonicWall Auth Bypass
SonicWall SQL Injection
Ivanti (MobileIron) Sentry Auth Bypass

22 Openfire Path Traversal
Ivanti MICS Scanning

21 TBK Vision DVR Auth Bypass

20

19

18 TurnitinBot
DomainStatsBot
SBA Research
Veeam Backup and Replication Credentials Retrieval

17

16

15 CrowdStrike Falcon Surface (Reposify)

14

13

12

11 PaperCut Path Traversal RCE

10

09 Apache ShenYu Admin Auth Bypass
GPTBot

08

07

06

05

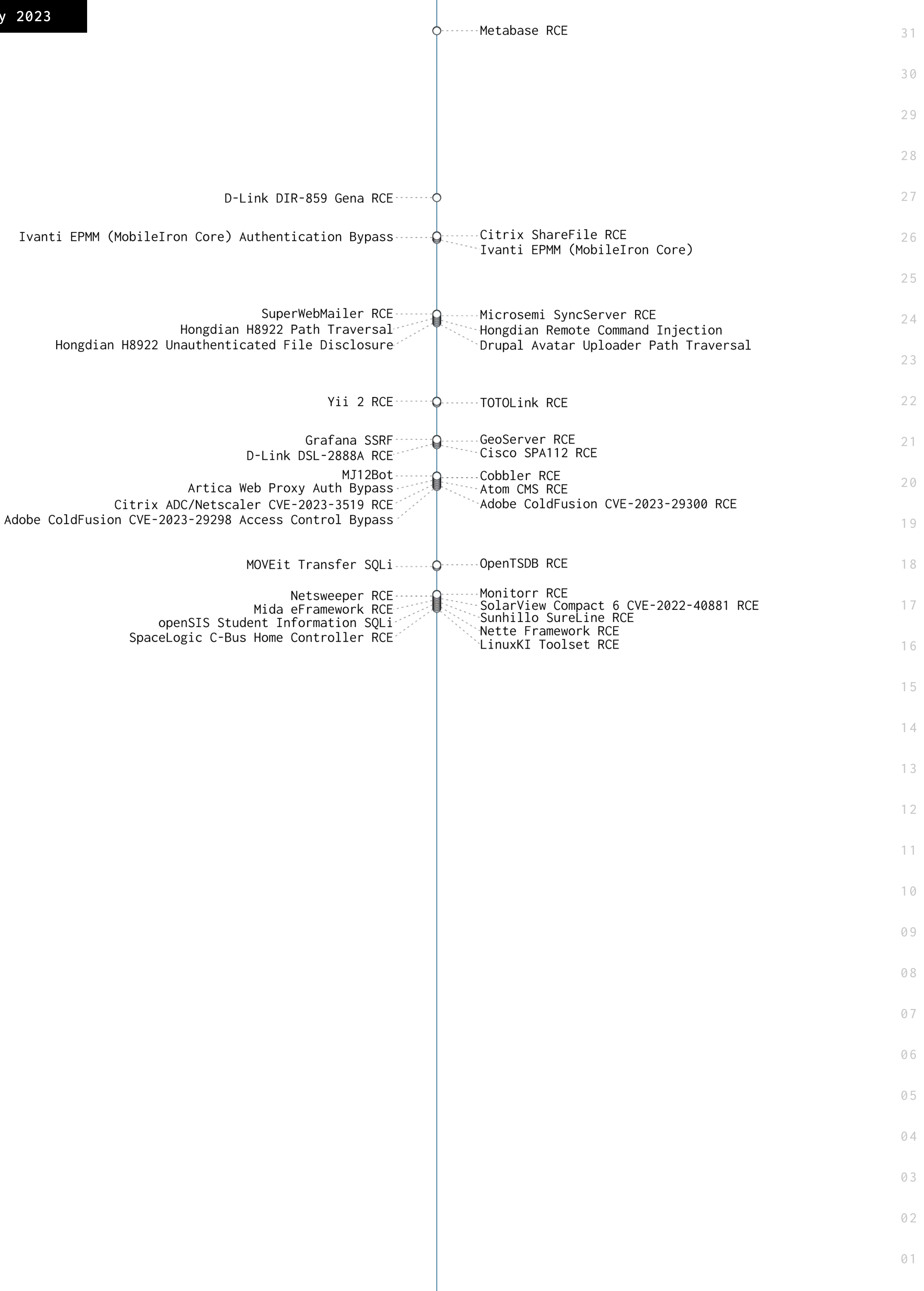
04

03

02

01

July 2023



Metabase RCE

D-Link DIR-859 Gena RCE

Ivanti EPMM (MobileIron Core) Authentication Bypass
Citrix ShareFile RCE
Ivanti EPMM (MobileIron Core)

SuperWebMailer RCE
Hongdian H8922 Path Traversal
Hongdian H8922 Unauthenticated File Disclosure
Microsemi SyncServer RCE
Hongdian Remote Command Injection
Drupal Avatar Uploader Path Traversal

Yii 2 RCE
TOTOLink RCE

Grafana SSRF
D-Link DSL-2888A RCE
GeoServer RCE
Cisco SPA112 RCE

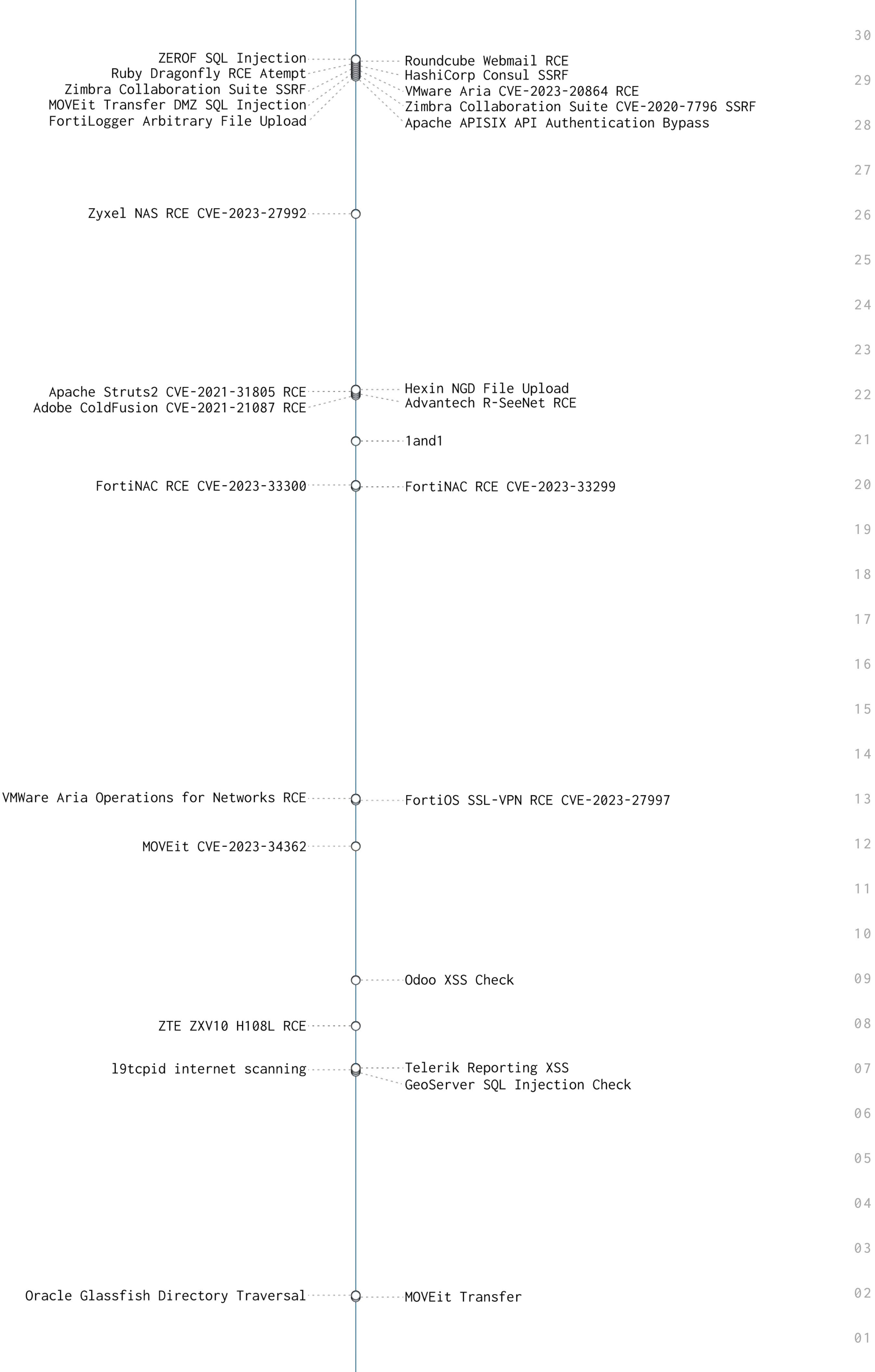
MJ12Bot
Artica Web Proxy Auth Bypass
Citrix ADC/Netscaler CVE-2023-3519 RCE
Adobe ColdFusion CVE-2023-29298 Access Control Bypass
Cobbler RCE
Atom CMS RCE
Adobe ColdFusion CVE-2023-29300 RCE

MOVEit Transfer SQLi
OpenTSDB RCE

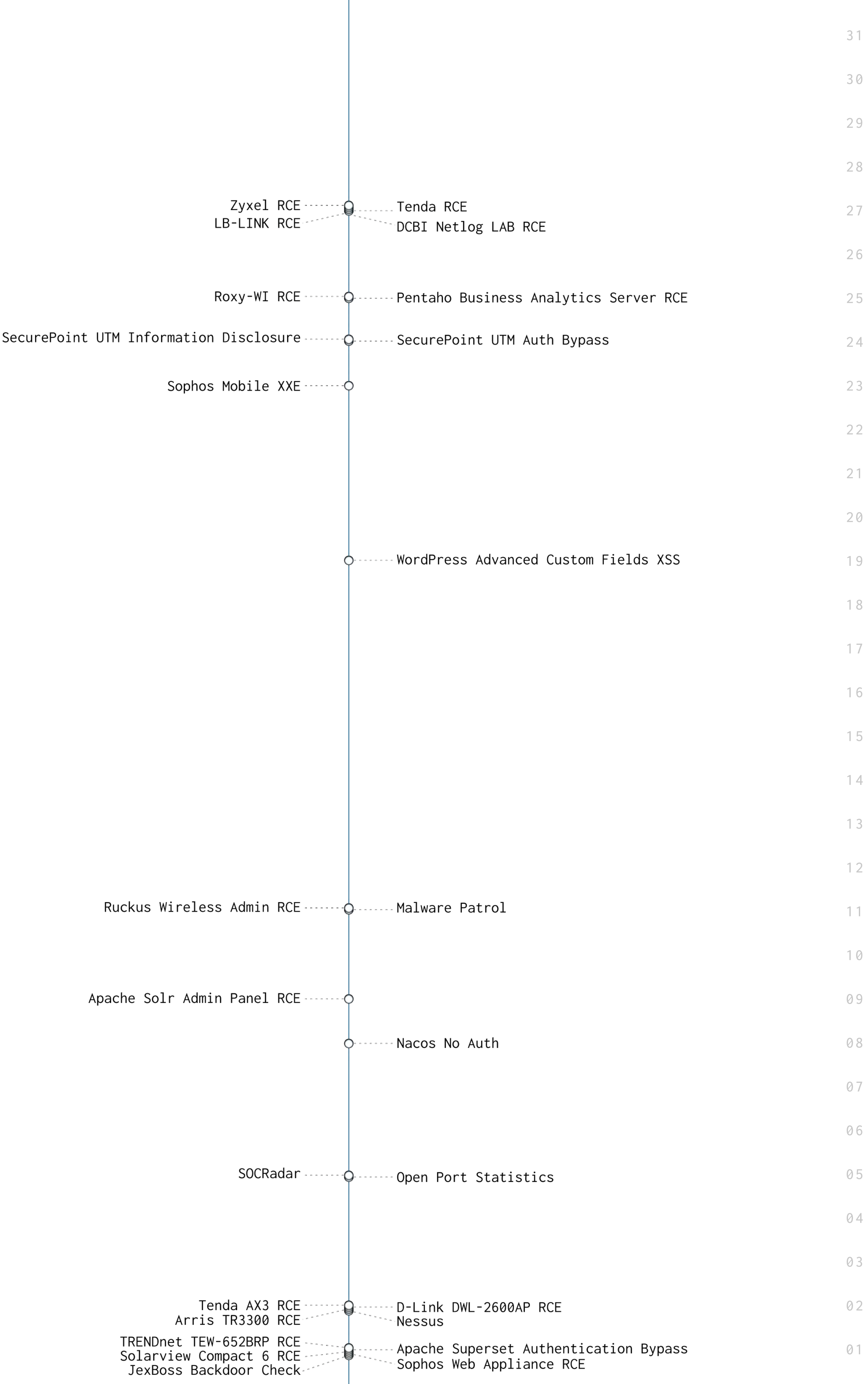
Netsweeper RCE
Mida eFramework RCE
openSIS Student Information SQLi
SpaceLogic C-Bus Home Controller RCE
Monitorr RCE
SolarView Compact 6 CVE-2022-40881 RCE
Sunhillo SureLine RCE
Nette Framework RCE
LinuxKI Toolset RCE

June 2023

APPENDIX B: 2023 TAG TIMELINE



May 2023



31

30

29

28

Zyxel RCE — Tenda RCE — 27
LB-LINK RCE — DCBI Netlog LAB RCE

26

Roxy-WI RCE — Pentaho Business Analytics Server RCE — 25

SecurePoint UTM Information Disclosure — SecurePoint UTM Auth Bypass — 24

Sophos Mobile XXE — 23

22

21

20

WordPress Advanced Custom Fields XSS — 19

18

17

16

15

14

13

12

Ruckus Wireless Admin RCE — Malware Patrol — 11

10

Apache Solr Admin Panel RCE — 09

Nacos No Auth — 08

07

06

SOCRadar — Open Port Statistics — 05

04

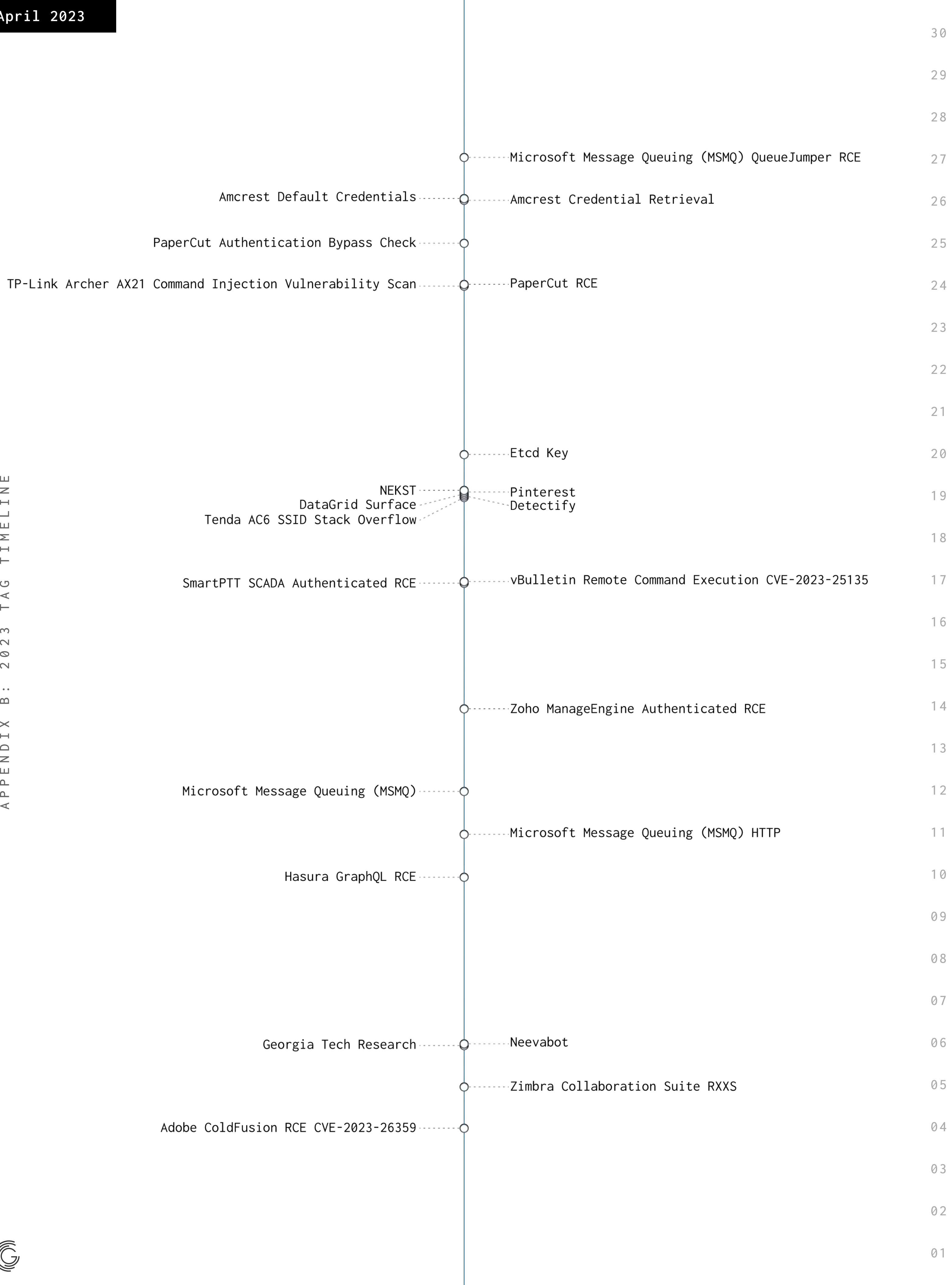
03

Tenda AX3 RCE — D-Link DWL-2600AP RCE — 02
Arris TR3300 RCE — Nessus

TRENDnet TEW-652BRP RCE — Apache Superset Authentication Bypass — 01
Solarview Compact 6 RCE — Sophos Web Appliance RCE
JexBoss Backdoor Check

April 2023

APPENDIX B: 2023 TAG TIMELINE



30

29

28

Microsoft Message Queuing (MSMQ) QueueJumper RCE

27

Amcrest Default Credentials

Amcrest Credential Retrieval

26

PaperCut Authentication Bypass Check

25

TP-Link Archer AX21 Command Injection Vulnerability Scan

PaperCut RCE

24

23

22

21

Etcd Key

20

NEKST

DataGrid Surface

Tenda AC6 SSID Stack Overflow

Pinterest

Detectify

19

18

SmartPTT SCADA Authenticated RCE

vBulletin Remote Command Execution CVE-2023-25135

17

16

15

Zoho ManageEngine Authenticated RCE

14

13

Microsoft Message Queuing (MSMQ)

12

Microsoft Message Queuing (MSMQ) HTTP

11

Hasura GraphQL RCE

10

09

08

07

Georgia Tech Research

Neevabot

06

Zimbra Collaboration Suite RXXS

05

Adobe ColdFusion RCE CVE-2023-26359

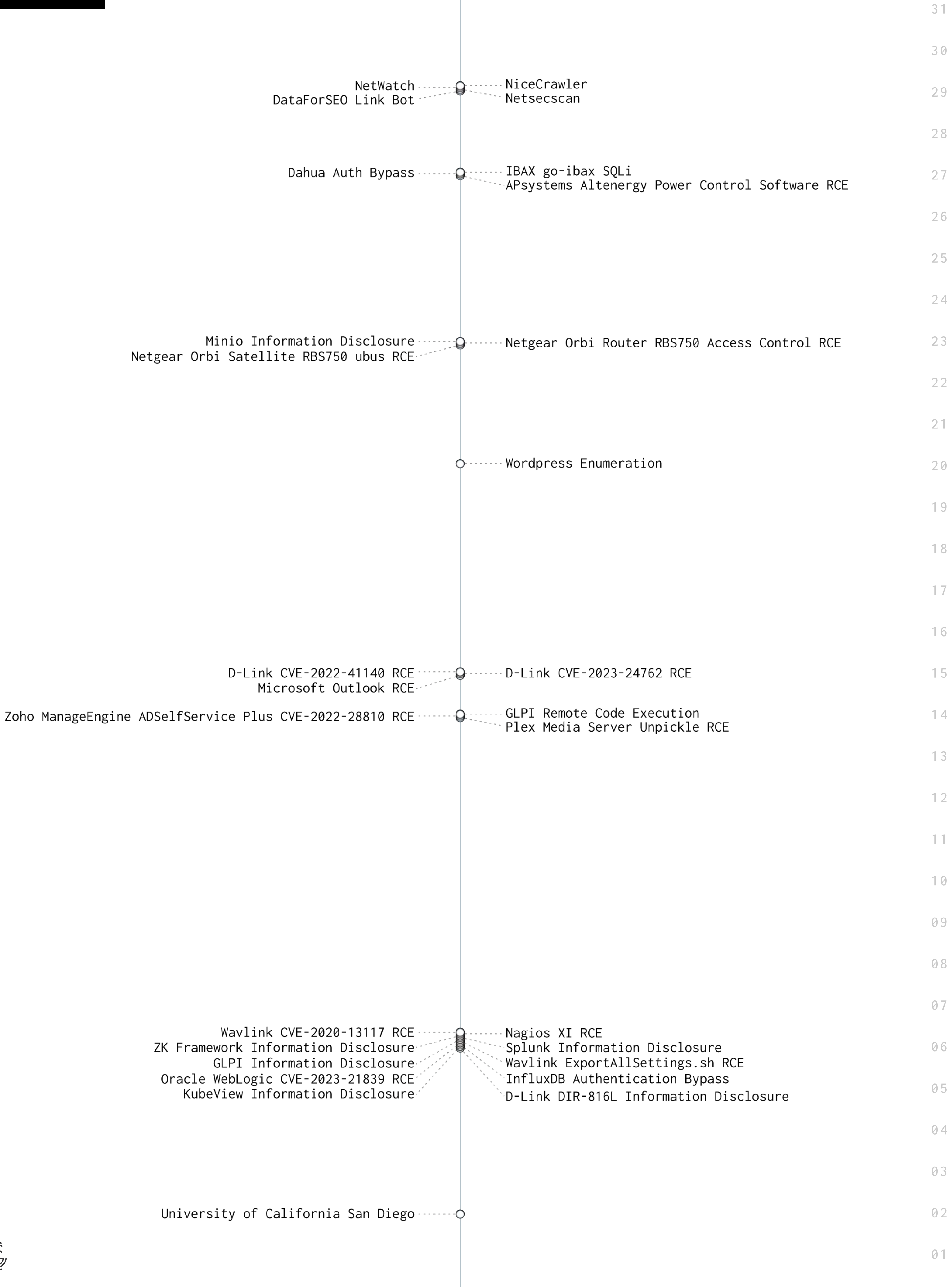
04

03

02

01

March 2023



NetWatch
DataForSEO Link Bot
NiceCrawler
Netsecscan

Dahua Auth Bypass
IBAX go-ibax SQLi
APsystems Altenergy Power Control Software RCE

Minio Information Disclosure
Netgear Orbi Satellite RBS750 ubus RCE
Netgear Orbi Router RBS750 Access Control RCE

Wordpress Enumeration

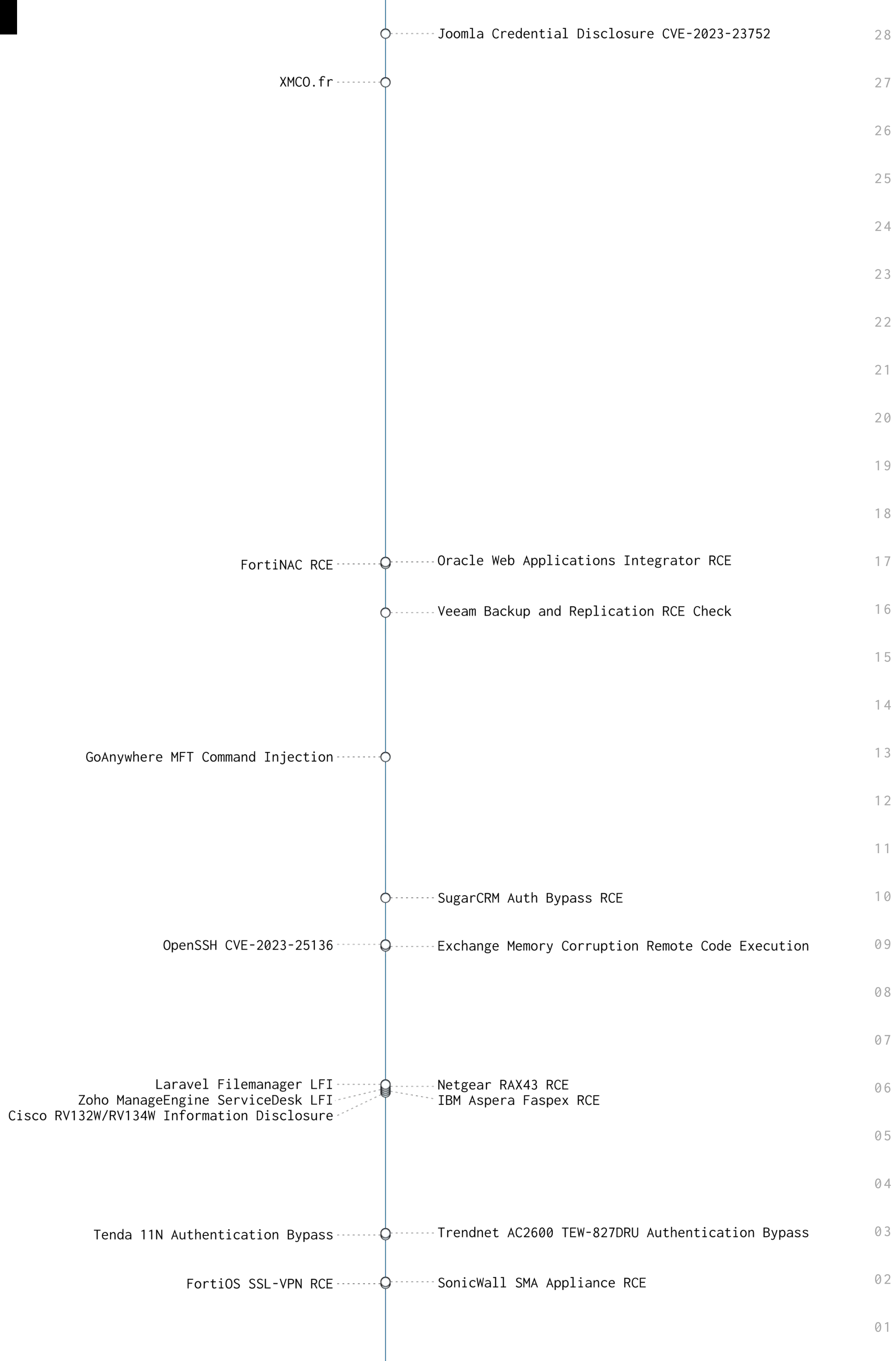
D-Link CVE-2022-41140 RCE
Microsoft Outlook RCE
D-Link CVE-2023-24762 RCE

Zoho ManageEngine ADSelfService Plus CVE-2022-28810 RCE
GLPI Remote Code Execution
Plex Media Server Unpickle RCE

Wavlink CVE-2020-13117 RCE
ZK Framework Information Disclosure
GLPI Information Disclosure
Oracle WebLogic CVE-2023-21839 RCE
KubeView Information Disclosure
Nagios XI RCE
Splunk Information Disclosure
Wavlink ExportAllSettings.sh RCE
InfluxDB Authentication Bypass
D-Link DIR-816L Information Disclosure

University of California San Diego

February 2023



28 Joomla Credential Disclosure CVE-2023-23752

27 XMCO.fr

26

25

24

23

22

21

20

19

18

17 FortiNAC RCE

17 Oracle Web Applications Integrator RCE

16 Veeam Backup and Replication RCE Check

15

14

13 GoAnywhere MFT Command Injection

12

11

10 SugarCRM Auth Bypass RCE

09 OpenSSH CVE-2023-25136

09 Exchange Memory Corruption Remote Code Execution

08

07

06 Laravel Filemanager LFI

06 Zoho ManageEngine ServiceDesk LFI

06 Cisco RV132W/RV134W Information Disclosure

06 Netgear RAX43 RCE

06 IBM Aspera Faspex RCE

05

04

03 Tenda 11N Authentication Bypass

03 Trendnet AC2600 TEW-827DRU Authentication Bypass

02 FortiOS SSL-VPN RCE

02 SonicWall SMA Appliance RCE

01

January 2023

		31
VMwarev Realize Log Insight Access Control Vulnerability	VMware vRealize Log Insight Directory Traversal	30
		29
		28
Apache CouchDB Remote Privilege Escalation	VMware vRealize Log Insight Information Disclosure	27
		26
		25
	Netcomm Wireless Router RCE	24
Tibco JasperSoft Path Traversal		23
		22
		21
		20
		19
	Merit LILIN DVR RCE	18
		17
		16
		15
		14
		13
Zoho ManageEngine RCE CVE-2022-47966	C-Data Unauthorized Web Management RCE	12
		11
TIBCO JasperReports Path Traversal	Lexmark MC3224adwe RCE	10
CentOS Web Panel RCE CVE-2022-44877		09
		08
		07
		06
	Fortinet SSL VPN Bruteforcer	05
Exim RCE		04
	Exchange OWASSRF Vuln	03
		02
		01

Appendix C: 2023 GreyNoise Tag ATT&CK Technique Mapping

T1574: Hijack Execution Flow

T1134: Access Token Manipulation

T1550: Use Alternate Authentication Material

T1548: Abuse Elevation Control Mechanism

T1505: Server Software Component

T1563: Remote Service Session Hijacking

T1546: Event Triggered Execution

2023 GreyNoise Tag	ATT&CK Technique
Adobe ColdFusion CVE-2023-29298 Access Control Bypass Attempt	T1546; T1574
Adobe ColdFusion RCE CVE-2023-26359 Attempt	T1546; T1574
Apache CouchDB Remote Privilege Escalation Attempt	T1548
Apache ShenYu Admin Auth Bypass Attempt	T1134; T1505; T1548; T1550; T1563
Atom CMS RCE Attempt	T1574
Cisco ASA Information Disclosure Attempt	T1574
Cisco IOS XE RCE Attempt	T1574
Cisco SPA112 RCE Attempt	T1134; T1550; T1574
Cisco VPN Router File Upload Attempt	T1574
CommVault CommCell Authentication Bypass Attempt	T1134; T1505; T1548; T1550; T1563
D-Link DAP-2020 Information Disclosure Attempt	T1574
D-Link DIR-816L Information Disclosure Attempt	T1134; T1505; T1548; T1550; T1563
Dahua Auth Bypass	T1134; T1505; T1548; T1550; T1563
FortiLogger Arbitrary File Upload Attempt	T1574
GLPI Remote Code Execution Attempt	T1574
Hongdian H8922 Unauthenticated File Disclosure Attempt	T1574
IBAX go-ibax SQLi Attempt	T1574

continued on next page

2023 GreyNoise Tag	ATT&CK Technique
InfluxDB Authentication Bypass Attempt	T1134; T1505; T1548; T1550; T1563
Ivanti EPMM (MobileIron Core) Authentication Bypass Attempt	T1134; T1505; T1548; T1550; T1563
JBoss Seam RCE Attempt	T1574
Jira Data Exposure Scanner	T1574
KubeOperator Unauth API Access Attempt	T1134; T1550; T1574
KubeView Information Disclosure Attempt	T1134; T1505; T1548; T1550; T1563
Lexmark Printers RCE Attempt	T1574
Microsoft Outlook RCE Attempt	T1134; T1550
Minio Information Disclosure Attempt	T1574
Monitorr RCE Attempt	T1574
Movable Type mt-upgrade.cgi RCE Attempt	T1134; T1505; T1548; T1550; T1563
Netcomm Wireless Router RCE Attempt	T1134; T1505; T1548; T1550; T1563
Oracle WebLogic CVE-2023-21839 RCE Attempt	T1574
PaperCut RCE Attempt	T1546; T1574
Qlik Sense Auth Bypass Attempt	T1574
Roxy-WI RCE Attempt	T1574
SonicWall Auth Bypass Attempt	T1134; T1505; T1548; T1550; T1563
Splunk Information Disclosure Attempt	T1574
SugarCRM Auth Bypass RCE Attempt	T1574
Tenda 11N Authentication Bypass Attempt	T1134; T1505; T1548; T1550; T1563
Trendnet AC2600 TEW-827DRU Authentication Bypass Attempt	T1134; T1505; T1548; T1550; T1563
VMware vRealize Log Insight Information Disclosure Attempt	T1574
Wester Bridge Cobub Razor 0.8.0 Physical Path Leakage Attempt	T1574
WordPress WPCargo Track & Trace RCE Attempt	T1574
ZK Framework Information Disclosure Attempt	T1574
jQuery-File-Upload Attempt	T1574
jQuery-File-Upload Attempt	T1134; T1505; T1548; T1550; T1563
phpThumb fltr RCE Attempt	T1574

Decoding 2023: A GreyNoise Retrospective on Internet Exploitation

About GreyNoise

GreyNoise helps security teams focus on threats that really matter, and ignore the ones that don’t. We collect, analyze and label data on IP addresses that scan and attack the entire internet, saturating security teams with alerts. This unique perspective helps analysts focus their time on targeted and emerging threats, and waste less time on irrelevant or harmless activity.

Get started for free ↗

Schedule a demo ↗