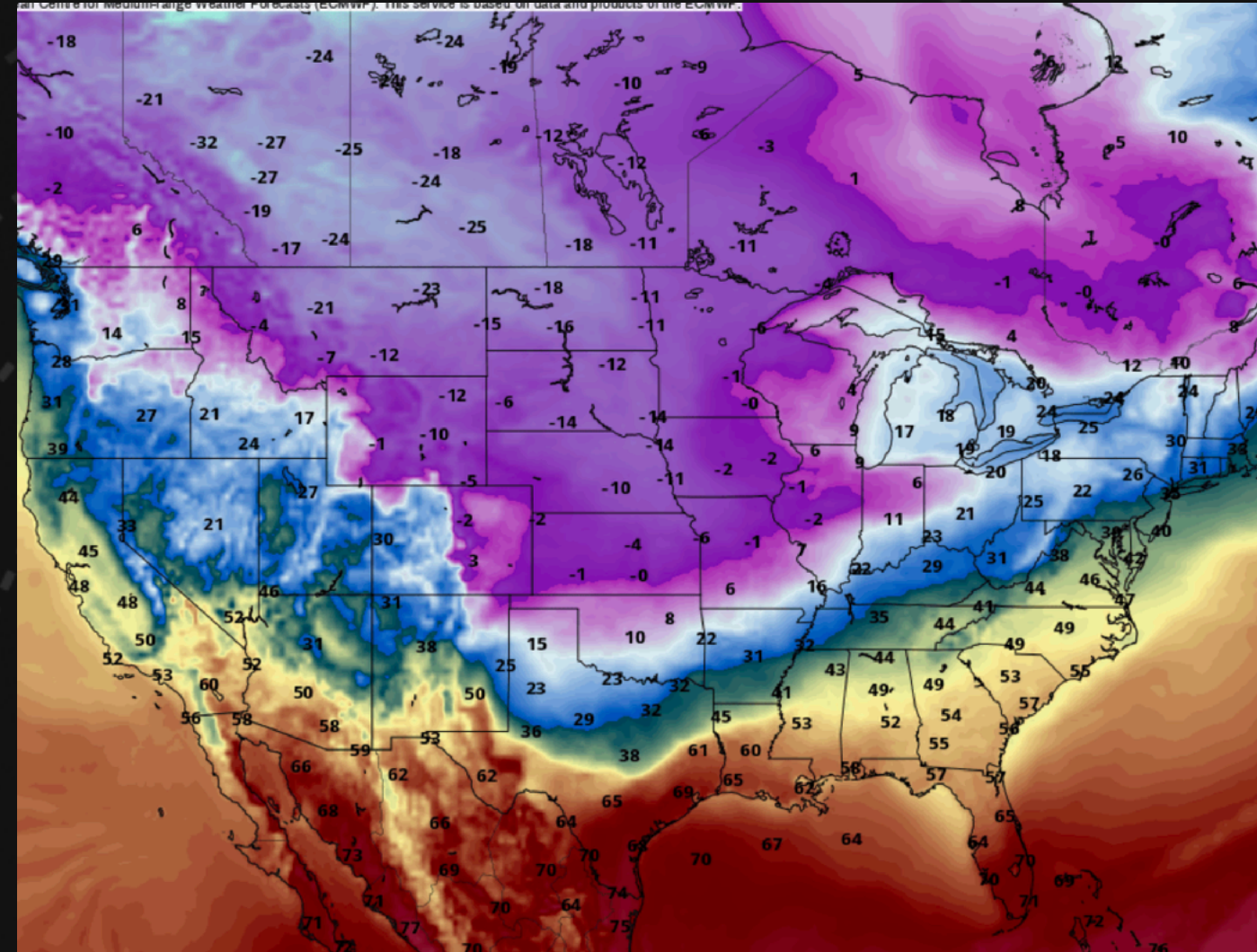


STORM ⚡ WATCH



Dateline



2024-01-09

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://pod.greynoise-storm.watch/>

<https://show.greynoise-storm.watch/>



SUBJECT

Andrew Morris

OCCUPATION

Founder and CEO

GreyNoise Intelligence

BACKGROUND

Morris has a strong background in offensive cyber operations, security research, and security engineering.

He has a stronger background in “hot takes” due to his Twitter/X addiction.

BREAKING NEWS



loanDepot

<https://www.bleepingcomputer.com/news/security/mortgage-firm-loandepot-cyberattack-impacts-it-systems-payment-portal/>

<https://www.sec.gov/Archives/edgar/data/1831631/000183163124000004/ldi-20240104.htm>



Shay M · Jan 6, 2024

@HoneysWorld007 · [Follow](#)

@loanDepot are your phones down???



loanDepot

@loanDepot · [Follow](#)

Good Morning Shay, loanDepot is experiencing a cyber incident, which is affecting our phone lines. We are working diligently to return to normal business operations as soon as possible. We apologize for the inconvenience.

11:33 AM · Jan 6, 2024



1




Reply



Share

[Read more on X](#)

Return Mail Processing
PO Box 999
Suwanee, GA 30024

6 1 1358 *****SNGLP
SAMPLE A. SAMPLE - All
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789


Re: Notice of Data Security Event

May 5, 2023

Dear Sample A. Sample:

At loanDepot, we take privacy very seriously. It is therefore important that we make you aware of data privacy issues that may affect you. Below you will find information about an incident that may have impacted your personal information and the steps we are taking to protect your information.

What Happened

On August 3, 2022, we observed anomalous activity on our IT network. We promptly launched an investigation and took a series of immediate steps designed to remediate the issue. loanDepot then engaged a leading cybersecurity firm to further secure our systems, determine the root cause, and further protect your information. loanDepot also reported the event to regulators.

loanDepot identified brief unauthorized access to a small number of internal accounts; this access was terminated and the incident was remediated within three hours. This incident has not affected your loan or our servicing of your account in any way. However, it is possible that the unauthorized actor could have accessed documents containing your personal information, as described below. There is no evidence that any personal data has been misused, but out of an abundance of caution, we wanted to notify anyone that may be affected.

What Information Was Involved

Our records indicate that your name and DATA may have been accessed.

What We Are Doing

We took a series of immediate steps to remediate the issue, engaged a leading cybersecurity firm to investigate the incident and further protect your information, and we implemented processes and protocols designed to prevent this, or something like this, from happening again.

What You Can Do

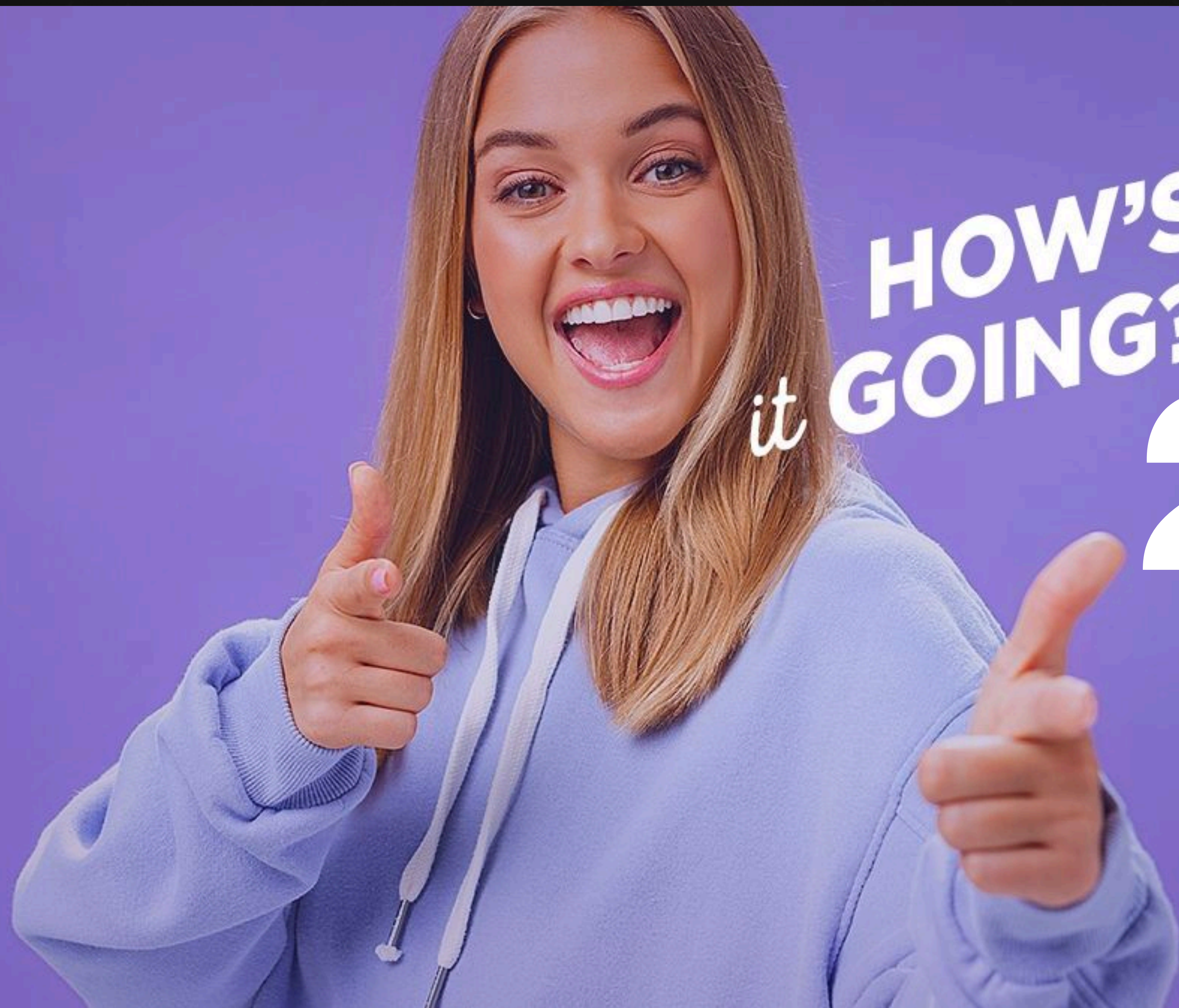
As discussed further below, we recommend you remain vigilant with respect to reviewing your account statements and credit reports. In addition, to help protect your identity from misuse, we are offering a complimentary 24 month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: August 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

R M A T C H

On August 3, 2022, we observed anomalous activity on our IT network. We promptly launched an investigation and took a series of immediate steps designed to remediate the issue. loanDepot then engaged a leading cybersecurity firm to further secure our systems, determine the root cause, and further protect your information. loanDepot also reported the event to regulators.

**NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING**



HOW'S
GOING?
it

2024



NEWS

23andMe blames “negligent” breach victims, says it’s their own fault

How ransomware could cripple countries, not just companies

Experts think 2023 was a record year for digital attacks



IMAGE: BEN DENZER

Threat Intelligence Report: The Potential For Global Disinformation and Misinformation Campaigns for 2024

<https://www.malwarebytes.com/blog/news/2024/01/23andme-blames-negligent-breach-victims-says-its-their-own-fault>
<https://www.economist.com/international/2023/12/31/how-ransomware-could-cripple-countries-not-just-companies>
<https://krypt3ia.wordpress.com/2024/01/04/threat-intelligence-report-the-potential-for-global-disinformation-and-misinformation-campaigns-for-2024/>

S T O R M ⚡ W A T C H

TOOL TIME





Document word or phrase ?

incident

Company name, ticker, CIK number or individual's name

Company name, ticker, CIK number or individual's name

Filing category

View all

Browse filing types

Filed date range

Custom

Filed from

2023-12-01

Filed to

2024-01-09

Principal executive offices in ?

View all

https://www.sec.gov/edgar/search/#/q=incident&dateRange=custom&startdt=2023-12-01&enddt=2024-01-09

Refine search results by:

Entity



Form



Principal executive offices located in



Click headings to show top filters.
Document counts shown in #

2,930 search results

Show Columns

☒ Filed ☒ Reporting for ☐ CIK ☐ Located ☐ Incorporated ☐ File number ☐ Film number

Form & File	Filed	Reporting for	Filing entity/person
8-K/A (Current report)	2023-12-01	2023-10-10	23andMe Holding Co. (ME)
8-K (Current report)	2023-12-18	2023-12-15	V F CORP (VFC)
8-K (Current report) EX-99.1	2023-12-06	2023-12-06	Fidelity National Financial, Inc. (FNF)
8-K (Current report)	2024-01-	2024-01-04	loanDepot Inc. (LDI)

S T O R M ⚡ W A T C H



Shameless Self-Promotion



Every Month, to Find Phishing Domains A

https://go.censys.com/JanuaryLunchandLearn_Registration.html

January 18, 2024 at 1:00pm ET

In this exclusive Censys Lunch and Learn webinar we will unravel the complexities of the vast digital landscape. In an era where the internet is both a treasure trove and a potential minefield, distinguishing between legitimate and malicious web pages has never been more challenging. The prevalence of technology has empowered cyber adversaries to swiftly deploy deceptive websites, posing a significant threat to organizations. Navigating this perilous terrain demands a proactive approach in identifying fake websites as they emerge and safeguarding your employees from potential cyber threats.

Join us as we delve into the intricacies of fuzzy matching where knowledge becomes your greatest defense. Learn how leveraging BigQuery's user-defined functions can empower you to identify phishing domains by finding websites that cunningly resemble your own. We will demonstrate the effectiveness of combining the capabilities of BigQuery with Censys' data, providing you with a powerful toolkit to proactively protect your organization. Through insightful queries and data analysis, discover how to stay one step ahead in the relentless battle against cyber threats. Don't miss this opportunity to fortify your defenses and secure your organization's digital presence!

Presenters:

Register Now

First Name:

Last Name:

Email:

Company:

Country:

Phone Number:

<https://www.greynoise.io/blog/cve-2022-1471-snakeyaml-deserialization-deep-dive>

LABS VULNERABILITIES

CVE-2022-1471: SnakeYAML Deserialization Deep Dive

The GreyNoise Team | January 3, 2024



<https://www.greynoise.io/blog/mining-the-undiscovered-country-with-greynoise-eap-sensors-f5-big-ip-edition>

LABS VULNERABILITIES

Mining The Undiscovered Country With GreyNoise EAP Sensors: F5 BIG-IP Edition

The GreyNoise Research Team | December 14, 2023



<https://www.greynoise.io/events/webinar-series-greynoise-tags-deep-dive>

GREYNOISE

WEBINAR SERIES

GreyNoise Tags Deep Dive 101, 201, 301

January 10th, 17th, 24th | 12:00pm CT / 1:00pm ET



S T O R M ⚡ W A T C H

- 🏷 Apache OFBiz Authentication Bypass Attempt (CVE-2023-51467)
- 🏷 YAML Insecure Deserialization (CVE-2022-1471, CVE-2023-43654, CVE-2022-21404, CVE-2022-31691, CVE-2021-41110, CVE-2021-21249, CVE-2020-1947, CVE-2016-8744, CVE-2016-9606, CVE-2017-3159)
- 🏷 GLPI CVE-2013-5696 Attempt (CVE-2013-5696)

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

S T O R M ⚡ W A T C H

[illegible]

**WE NEED
TO TALK
ABOUT
KEY**

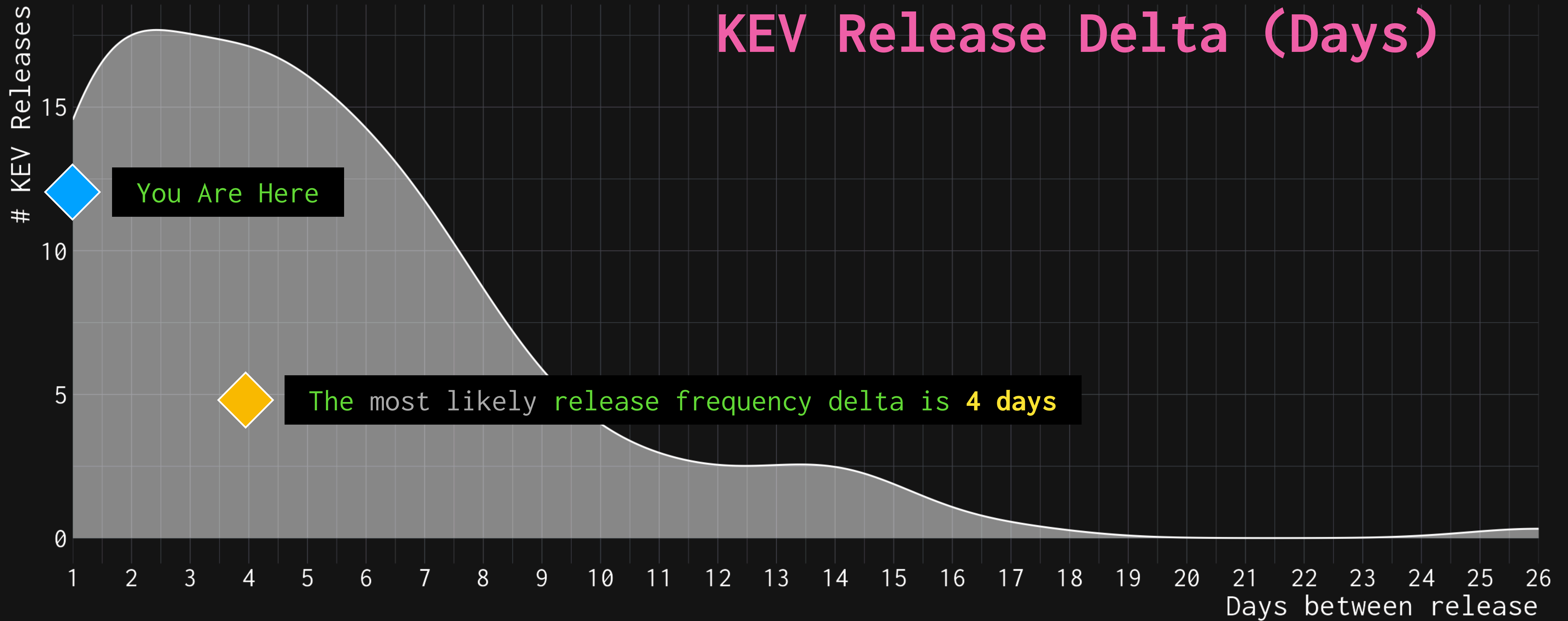


It Has Been

1

Days Since The
Last KEV Release

<https://observablehq.com/@greynoise/greynoise-tags>



<https://en.wikipedia.org/wiki/Trimean>

S T O R M ⚡ W A T C H

- 🏷️ CVE-2023-23752: Joomla! Improper Access Control
- 🏷️ CVE-2023-27524: Apache Superset Insecure Default Resource Initialization
- 🏷️ CVE-2023-29300: Adobe ColdFusion Deserialization of Untrusted Data
- 🕒 CVE-2016-20017: D-Link DSL-2750B Devices Command Injection
- 🕒 CVE-2023-38203: Adobe ColdFusion Deserialization of Untrusted Data
- ❌ CVE-2023-41990: Apple Multiple Products Code Execution Vulnerability

+ Four More From Long Ago