

S T O R M W Ø T C H

Dateline: 2023-12-19



GREYNOISE
LABS

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/>



It's all good



GREYNOISE
LABS

STORM ⚡ WATCH

THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware



This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6lrbvtflruqfc5ep7elodlad.onion (Tor browser required).

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit <https://rfj.tips/SDT55f>.



Newsroom

Press Releases

Speeches and
Statements

SEC Stories

Securities Topics

Media Kit

Press Contacts

Events

Webcasts

Media Gallery

► RSS Feeds

► Social Media

Statement

<https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214>

Cybersecurity Disclosure

Erik Gerding

Director, Division of Corporation Finance

Dec. 14, 2023

As is customary, I am expressing my views today in my official capacity as Director of the SEC's Division of Corporation Finance, and my views do not necessarily reflect the views of the Commission, any of the Commissioners, or any other Commission staff.

In July of this year, the Commission adopted final rules that will require public companies to disclose both material cybersecurity incidents they experience and, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.^[1] These rules will provide investors with timely, consistent, and comparable information about an important set of risks that can cause significant losses to public companies and their investors. This disclosure can help investors evaluate those risks as they make investment and voting decisions.

In recommending these final rules, the staff of the Division of Corporation Finance, together with staff from around the Commission, carefully considered the comments the Commission received^[2] on the March 2022 proposed rules.^[3] The Commission took these comments—including concerns about compliance and threat actors—into account in deciding to make changes from the proposal and in fashioning a set of rules that advance our goals of protecting investors and facilitating capital formation.





Cybersecurity Incident Disclosure

Disclose material cybersecurity incidents within four business days after determining the incident's materiality.

Describe the nature, scope, timing, and material impact of the incident on the company's financial condition and operations.

Avoid disclosing specific technical details that could compromise response or remediation efforts.

Media Gallery

▶ RSS Feeds

▶ Social Media

In recommending these final rules, the staff of the Division of Corporation Finance, together with staff from around the Commission, carefully considered the comments the Commission received^[2] on the March 2022 proposed rules.^[3] The Commission took these comments—including concerns about compliance and threat actors—into account in deciding to make changes from the proposal and in fashioning a set of rules that advance our goals of protecting investors and facilitating capital formation.

Annual Cybersecurity Risk Management Disclosure

Report annually on cybersecurity risk management, strategy, and governance.

Focus on management's role in assessing and managing cybersecurity risks.

Disclose if any management positions or committees are responsible for cybersecurity threats and their relevant expertise.

Describe the board's oversight of cybersecurity risks and, if applicable, the relevant board committee's role.

Provide a non-exclusive list of disclosure items, acknowledging diverse approaches to cybersecurity.



National Security and Public Safety Delay Provision

Allow for delayed reporting of cybersecurity incidents that could pose a substantial risk to national security or public safety, contingent on written notification by the Attorney General.

Media Gallery

▶ RSS Feeds

▶ Social Media

disclosure can help investors evaluate those risks as they make investment and voting decisions.

In recommending these final rules, the staff of the Division of Corporation Finance, together with staff from around the Commission, carefully considered the comments the Commission received^[2] on the March 2022 proposed rules.^[3] The Commission took these comments—including concerns about compliance and threat actors—into account in deciding to make changes from the proposal and in fashioning a set of rules that advance our goals of protecting investors and facilitating capital formation.

What We Investigate

Terrorism | Counterintelligence | **Cyber Crime** | Public Corruption | Civil Rights | Organized Crime | White-Collar Crime | Violent Crime | More

News | Most Wanted | Business and Industry Partners | **FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements**

FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements

The Securities and Exchange Commission's new requirements for companies to disclose material cybersecurity incidents take effect on December 18, 2023. The FBI, in coordination with the Department of Justice, is providing guidance on how victims can request disclosure delays for national security or public safety reasons. The FBI recommends all publicly traded companies establish a relationship with the cyber squad at their [local FBI field office](#).

You can click on the buttons at the bottom of this page to read [guidance on requesting a delay and providing necessary information to the FBI](#), to [view the SEC Rule](#), to view [the Justice Department's material cybersecurity incident delay determinations guidelines](#), and to read [the FBI's Policy Notice](#) about how victim requests are processed.

The FBI strongly encourages companies to contact the FBI directly or through the U.S. Secret Service (USSS), another federal law enforcement agency, the Cybersecurity and Infrastructure Security Agency (CISA), or another sector risk management agency soon after a registrant believes disclosure of a newly-discovered cybersecurity incident may pose a substantial risk to national security or public safety. This early outreach allows the FBI to familiarize itself with the facts and circumstances of an incident before the company makes a materiality determination. If the victim of a cyber intrusion engages with the FBI or another U.S. government agency, this engagement doesn't trigger a determination of materiality. However, it could assist with the FBI's review if the company determines that a cyber incident is material and seeks a disclosure delay.

<https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements>



Request a Delay*



SEC Rule



FBI Policy Notice



DOJ Memo



BREAKING NEWS

Notice To Customers of Data Security Incident

Notice of Data Security Incident

We are notifying you of a recent data security incident involving your personal information. This notice explains the incident, steps Xfinity has taken to address it, and guidance on what you can do to protect your personal information.

What Happened? On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.

However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.

What Information Was Involved? On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.

What We Are Doing. To protect your account, we have proactively asked you to reset your password. The next time you login to your Xfinity account, you will be prompted to change your password, if you haven't been asked to do so already.

What You Can Do. We strongly encourage you to enroll in [two-factor or multi-factor authentication](#). While we advise customers not to re-use passwords across multiple accounts, if you do use the same information elsewhere, we recommend that you change the information on those other accounts, as well. You can review the "Additional Information" section below for information on how you can further protect your personal information.

More Information. If you have additional questions, please contact IDX, Xfinity's incident response provider managing customer notifications and call center support, at 888-799-2560 toll-free Monday through Friday from 9:00 AM to 9:00 PM EST, excluding federal holidays. More information is available on the Xfinity website at www.xfinity.com/dataincident.

We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter. We remain committed to continue investing in technology, protocols and experts dedicated to helping to protect your data and keeping you, our customer, safe.

Sincerely,

Xfinity

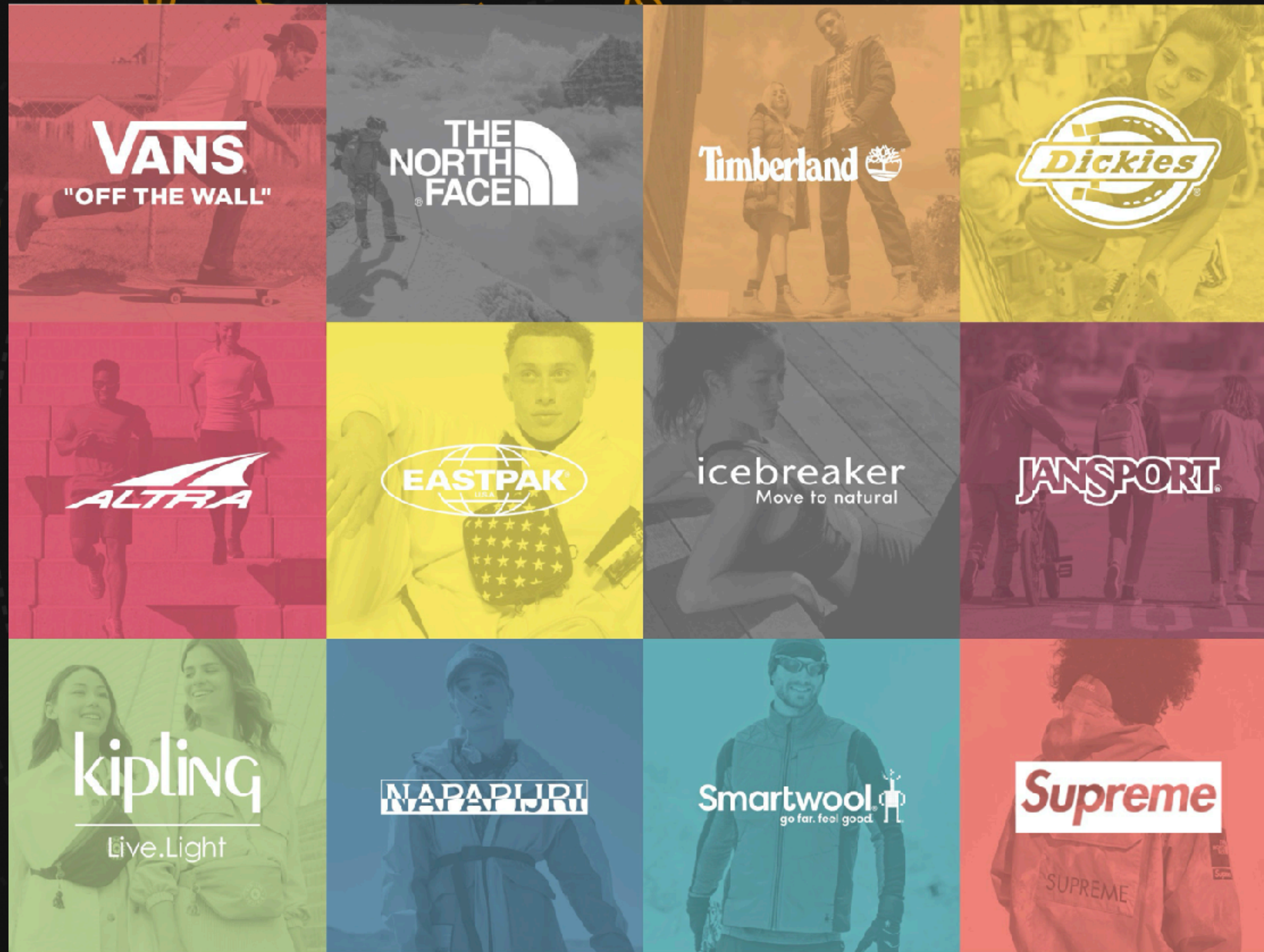
Additional Information

In general, you should remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You are entitled to a free copy of your credit report annually. To obtain your credit report, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or mail an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report



<https://assets.xfinity.com/assets/dotcom/learn/Notice To Customers of Data Security Incident.pdf>

<https://ir.stockpr.com/vfc/sec-filings-email/content/0000950123-23-011228/d659095d8k.htm>

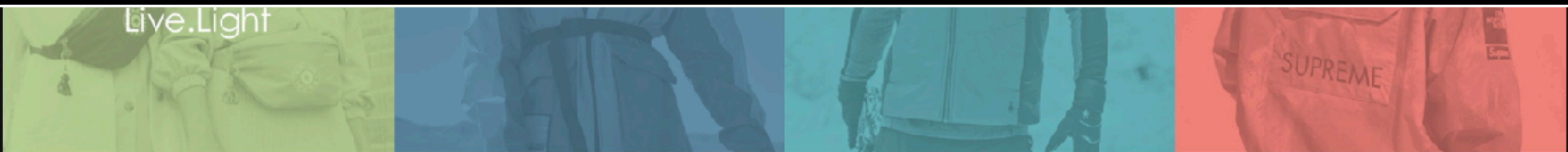



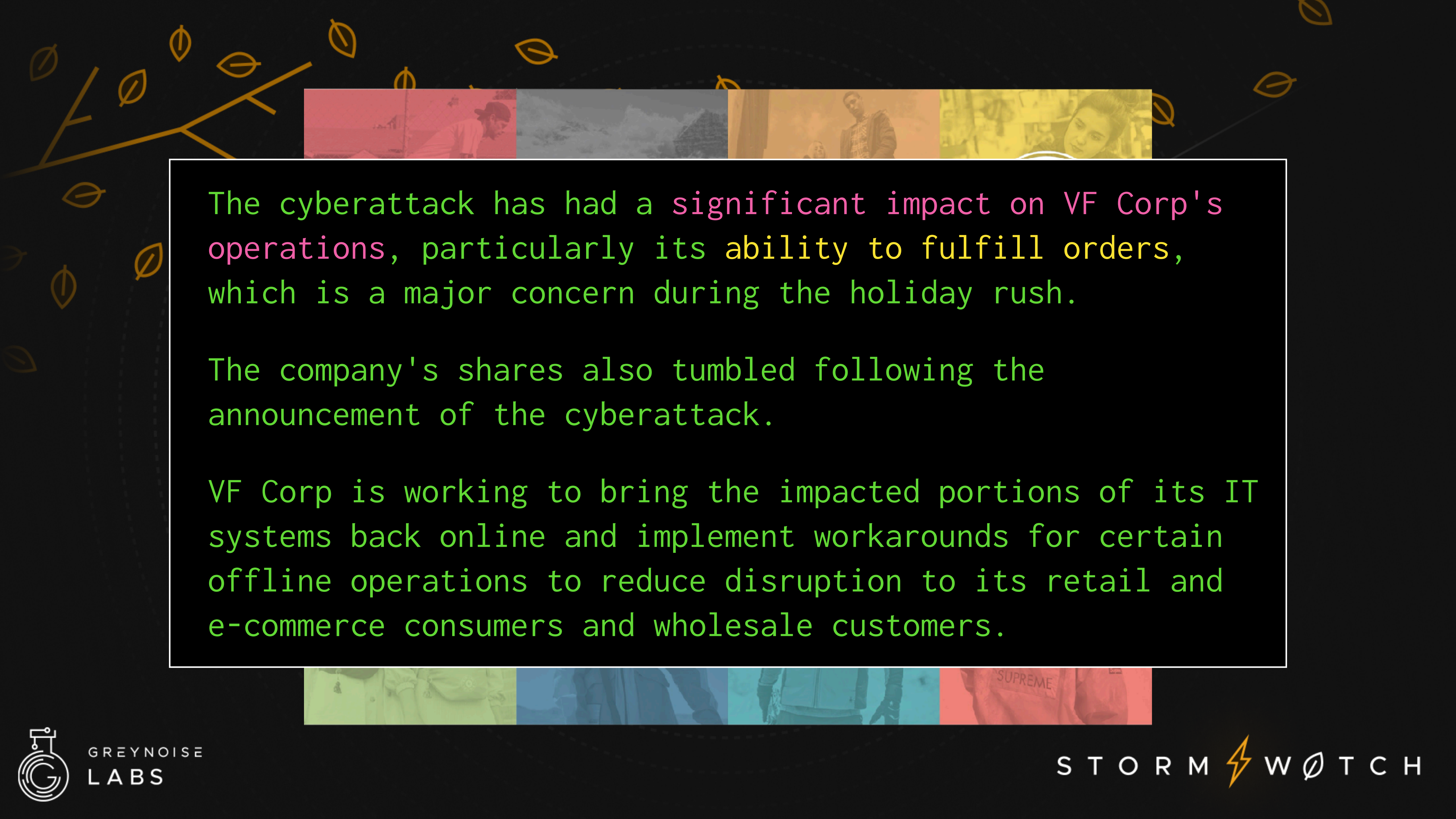


VF Corporation suffered a significant cyberattack on December 13, 2023.

The incident was detected when unauthorized activity was observed on a portion of the company's IT systems, leading to a shutdown of some systems.

The cyberattack disrupted VF Corp's business operations by encrypting some of its IT systems and stealing data, including personal data.

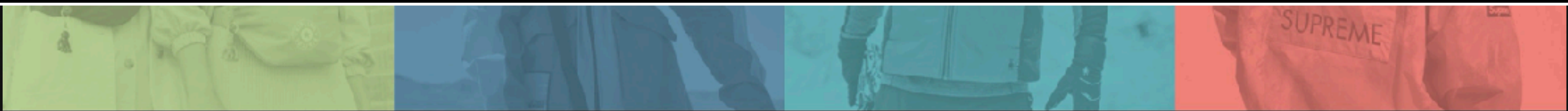



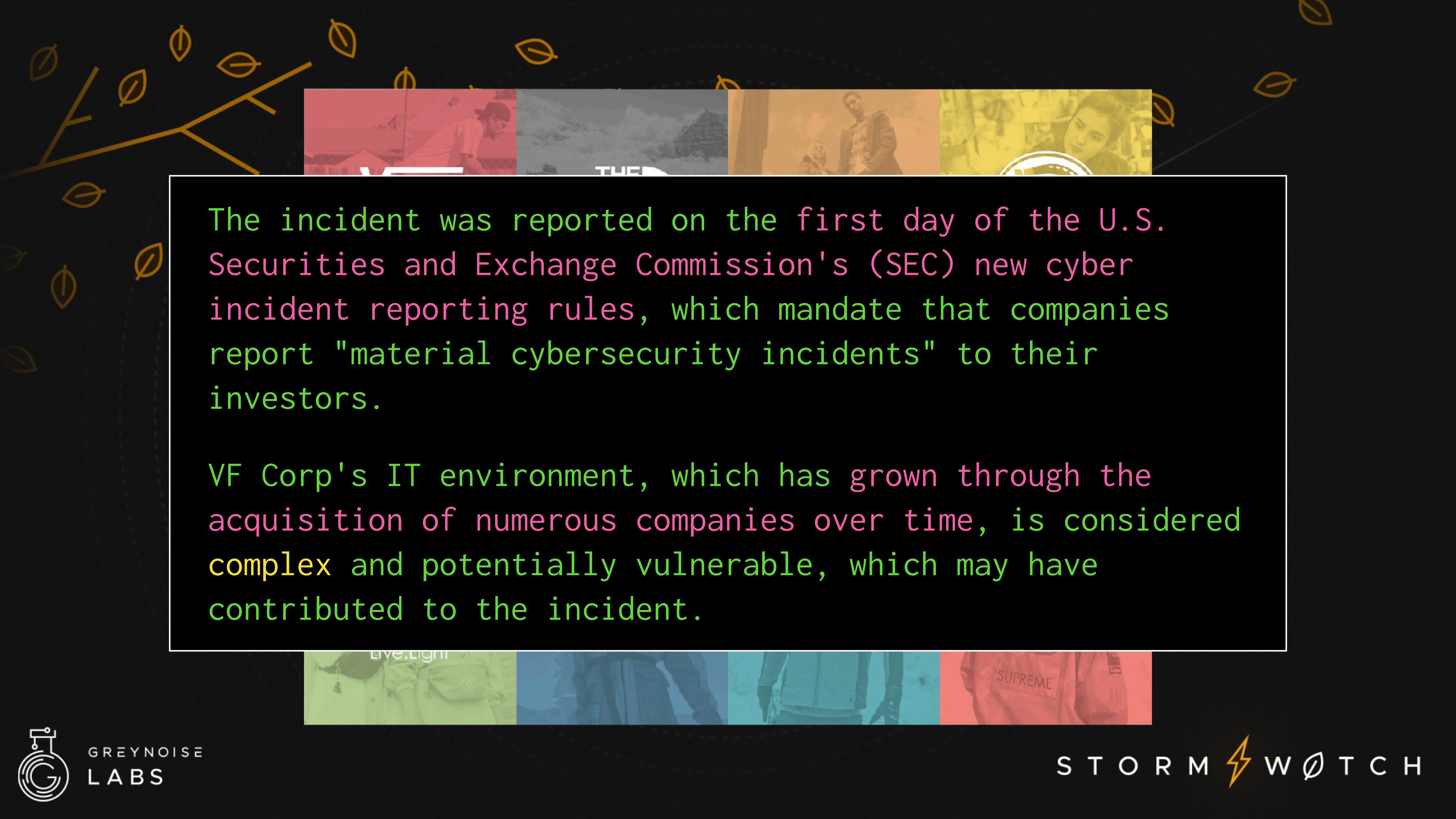


The cyberattack has had a significant impact on VF Corp's operations, particularly its ability to fulfill orders, which is a major concern during the holiday rush.

The company's shares also tumbled following the announcement of the cyberattack.

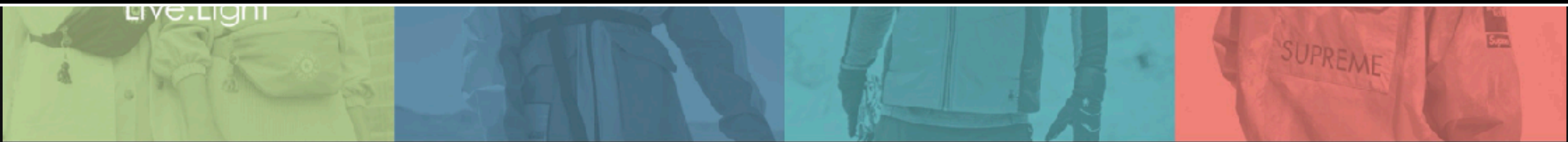
VF Corp is working to bring the impacted portions of its IT systems back online and implement workarounds for certain offline operations to reduce disruption to its retail and e-commerce consumers and wholesale customers.





The incident was reported on the first day of the U.S. Securities and Exchange Commission's (SEC) new cyber incident reporting rules, which mandate that companies report "material cybersecurity incidents" to their investors.

VF Corp's IT environment, which has grown through the acquisition of numerous companies over time, is considered complex and potentially vulnerable, which may have contributed to the incident.





TOOL TIME



GREYNOISE
LABS

STORM ⚡ WATCH

<https://viss.zoom.com/calculator/>

Infrastructure
Critical

100

Tenancy
Medium

51.02

Data
Critical

100

VISS
Critical

100

[Reset](#)

Platform Impacted ?

Platform Impacted

Zoom Infrastructure ▼

Platform Impact ?

Confidentiality

Unrestricted RCE ▼

Integrity

Unrestricted RCE ▼

Availability

Single Service on Sin... ▼

Tenancy ?

Infrastructure

Single ▼

Software

Single ▼

Database

N/A ▼

Tenants Impacted ?

Tenants Impacted

One ▼

Data Impact ?

Confidentiality

Multiple Organization... ▼

Integrity

None ▼

Availability

None ▼

Data Classification ?

Data Classification

Customer - Confident... ▼

Compensating Controls ?

Compensating Controls

N/A ▼

Infrastructure
Critical

100

Tenancy
Medium

51.02

Data
Critical

100

VISS
Critical

100

Reset

VISS uses thirteen metrics to evaluate the impact of vulnerabilities, such as Platform Impacted (PLI), Platform Confidentiality Impact (ICI), Platform Integrity Impact (III), Platform Availability Impact (IAI), Infrastructure Tenancy (ITN), Software Tenancy (STN), Data Tenancy (DTN), Tenants Impacted (TIM), Data Confidentiality Impact (DCI), Data Integrity Impact (DII), Data Availability Impact (DAI), and Upstream Compensating Controls (UCI)

Data Classification ?

Data Classification

Customer - Confident... ▼

Compensating Controls ?

Compensating Controls

N/A ▼



Infrastructure
Critical

100

Tenancy
Medium

51.02

Data
Critical

100

VISS
Critical

100

The VISS calculation produces a score ranging from 0 to 100, which can then be modified by applying the Compensating Controls metric.

A VISS score is represented as a vector string, a compressed textual representation of the metrics and corresponding values used to derive the score.

VISS:0.06:PLI:ZI/ICI:ICURCE/III:N/IAI:N/ITN:S/STN:S/DTN:NA/
TIM:0/DCI:M0/DII:N/DAI:N/DCL:C/UCI:NA

Data Classification ?

Customer - Confidential

Compensating Controls ?

Compensating Controls

N/A

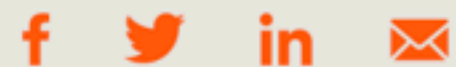


Shameless Self-Promotion

<https://censys.com/cve-2023-42793-jetbrains-teamcity/>

CVE-2023-42793: JetBrains TeamCity RCE Vulnerability

SHARE



DECEMBER 15, 2023

Tags: [Censys Search](#), [CVE](#), [Rapid response](#), [Vulnerabilities](#)

In recent months a vulnerability in the JetBrains TeamCity software ([CVE-2023-42793](#)) has been abused to achieve unauthenticated remote code execution in affected servers. Researchers at Rapid7 have analyzed the vulnerability and [created a Metasploit module](#) to

ABOUT THE AUTHOR



Aidan Holland
Security Researcher

Aidan is a Security



<https://www.greynoise.io/blog/a-day-in-the-life-of-a-greynoise-researcher-the-path-to-understanding-the-remote-code-execution-vulnerability-apache-cve-2023-50164-in-apache-struts2>

LABS

A Day In The Life Of A GreyNoise Researcher: The Path To Understanding The Remote Code Execution Vulnerability Apache (CVE-2023-50164) in Apache Struts2

The GreyNoise Team | December 13, 2023



Apache Struts2

CVE-2023-50164



<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



- WordPress Backup Migration RCE Attempt (CVE-2023-6553)
- 3CX CRM SQL Injection Attempt (CVE-2023-49954)
- WuzhiCMS CVE-2018-11528 SQLi Attempt (CVE-2018-11528)

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

**WE NEED
TO TALK
ABOUT
KEY**



It Has Been

8

Days Since The
Last KEV Release

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



CYBERSECURITY ADVISORY

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>

#StopRansomware: Play Ransomware

Release Date: December 18, 2023

Alert Code: AA23-352A

RELATED TOPICS: [CYBER THREATS AND ADVISORIES](#), [MALWARE](#), [PHISHING](#), AND [RANSOMWARE](#)



ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM PLAY RANSOMWARE:

1. Prioritize remediating known exploited vulnerabilities.
2. Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
3. Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.





The Play ransomware group has been targeting businesses and critical infrastructure in North America, South America, and Europe since June 2022, with approximately 300 affected entities known as of October 2023.

The group employs a double-extortion model, encrypting systems after exfiltrating data

1. Prioritize remediating known exploited vulnerabilities.
2. Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
3. Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.





The Play ransomware group typically gains initial access to victim networks through the abuse of valid accounts and exploitation of public-facing applications, specifically known FortiOS and Microsoft Exchange vulnerabilities.

They use tools like AdFind, Grixba, GMER, IOBit, and PowerTool for discovery, defense evasion, and lateral movement.

The group encrypts files using AES-RSA hybrid encryption and adds a .play extension to file names.

3. Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.





<https://www.cisa.gov/news-events/alerts/2023/12/15/cisa-secure-design-alert-urges-manufacturers-eliminate-default-passwords>

ALERT

CISA Secure by Design Alert Urges Manufacturers to Eliminate Default Passwords

Release Date: December 15, 2023

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)



Today, CISA published guidance on [How Manufacturers Can Protect Customers by Eliminating Default Passwords](#) as a part of our new Secure by Design (SbD) Alert series.

This SbD Alert urges technology manufacturers to proactively eliminate the risk of default password exploitation by implementing principles one and three of the joint guidance, [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software](#):

- Take ownership of customer security outcomes.

