VULCAN.

VOYAGER18

Q4 2023
Vulnerability Watch

Quarterly trends, themes and insights from
the world of cyber security vulnerabilities
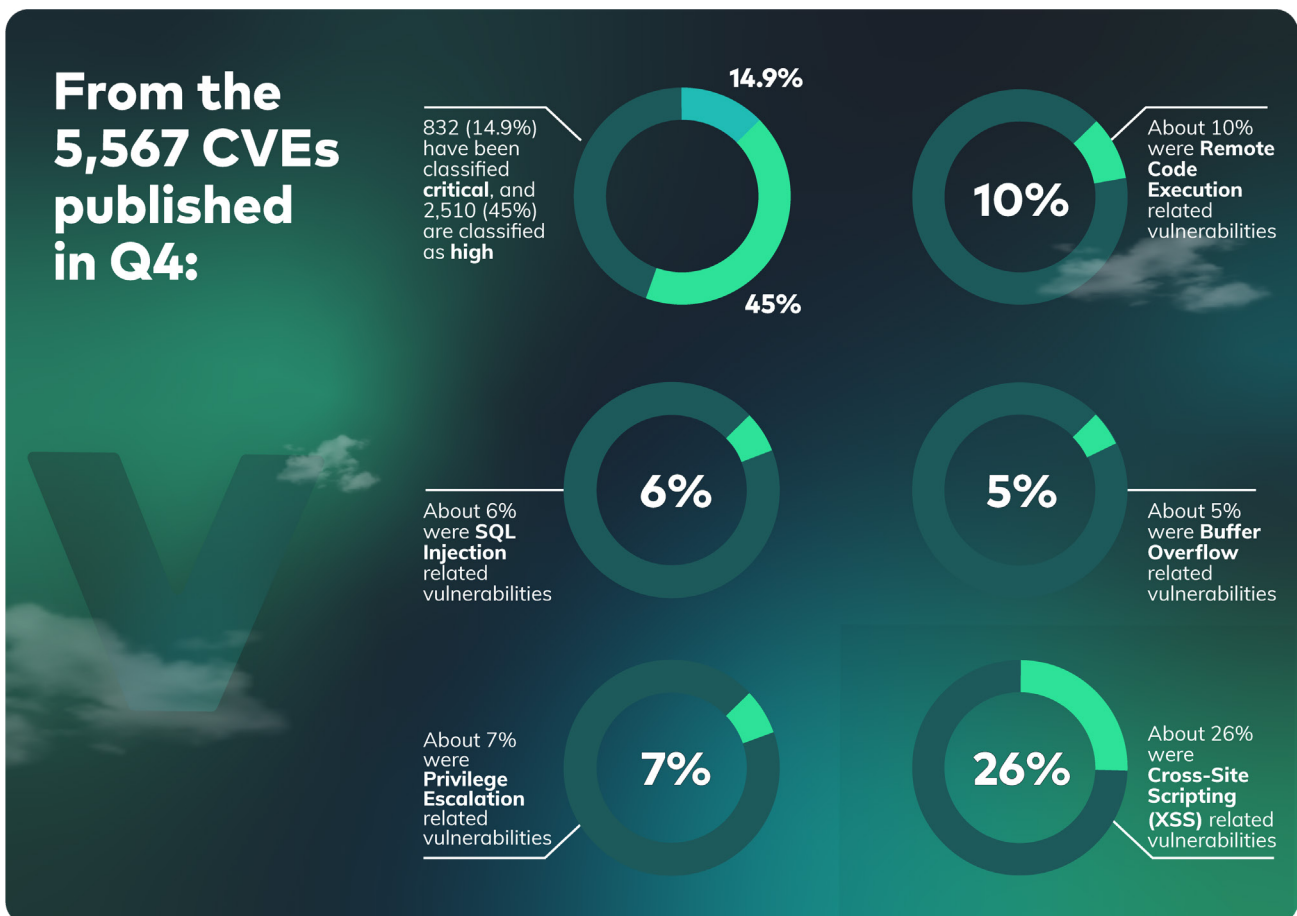
Table of contents

Introduction

This report highlights significant vulnerabilities identified in the fourth quarter of 2023. Updated through December 26th, it describes the possible repercussions of these vulnerabilities and provides actionable insights for organizations to bolster their vulnerability risk management practices. As with the previous iterations from Q1, Q2 and Q3, while the report offers detailed technical information on CVEs, it also delves deeper than just the Common Vulnerability Scoring System (CVSS) severity rating by incorporating data about their Exploitability Score (EPSS) and their listing in the Cybersecurity and Infrastructure Security Agency (CISA) catalog, along with other pertinent information.

The story of Q4 2023

The past quarter, and indeed all of 2023, have brought up some notable points of interest to be aware of as we head into 2024. Below are just some of our findings.

From the 5,567 CVEs published in Q4:

832 (14.9%) have been classified **critical**, and 2,510 (45%) are classified as **high**

14.9%

45%

About 10% were **Remote Code Execution** related vulnerabilities

10%

About 6% were **SQL Injection** related vulnerabilities

6%

About 5% were **Buffer Overflow** related vulnerabilities

5%

About 7% were **Privilege Escalation** related vulnerabilities

7%

About 26% were **Cross-Site Scripting (XSS)** related vulnerabilities

26%

Meanwhile, we pinpointed a number of prominent trends for Q4:

AI continues to confound

Like many in our industry, we have been preoccupied with the emerging opportunities and challenges presented by the rise of generative AI. Our extensive research into this topic has yielded a number of practical insights, most notably through our work in discovering what we termed AI package hallucination (more below). As a fast-developing technology, our research here is far from over, but the below summaries mark the work we've completed thus far.

AI-generated threats

AI's capability to create advanced malware and facilitate social engineering represents a significant new threat. AI can tailor phishing emails and malicious software to specific targets, increasing the effectiveness of cyber-attacks.

Certainly, crafting a sensitive email in this circumstance is important. Below is a sample email that you can use as a guideline:

Subject: Loss in the Family: Uncle [Uncle's Name] Has Passed Away

Dear [Relative's Name],

I hope this email finds you well, although I regret to say that I'm writing to share some sad news. Uncle [Uncle's Name] passed away last [day of the week], and it has been a difficult time for all of us. We are in the midst of making funeral arrangements and supporting each other as best we can during this challenging period.

I wanted to reach out to you personally as I know you had a special relationship with him. I also understand that it's been some time since we were last in touch, but family is important, especially at times like these.

The funeral service will be held on [date] at [location]. You are, of course, more than welcome to join us as we say our final goodbyes and celebrate his life. If you can't make it, we completely understand given the distance and any other commitments you may have.

It would mean a lot to us, however, if we could reconnect in the near future. Losses like this remind us how important it is to keep our loved ones close, even if they are far away in terms of distance.

Please feel free to reach out to me for any details or if you just want to talk. I'm here for you, as I know you would be for me.

AI Package Hallucination

A novel attack method where AI systems are tricked into suggesting nonexistent software resources that contains malware. This technique exploits AI's understanding and response generation, leading to potential cyber security risks.

```
{
  "role": "user",
  "content": "can you please provide me more npm packages to install that do it?"
},
{
  "role": "assistant",
  "content": "There are several npm packages available that allow you to interact with ArangoDB in Node.js. Here are a few options:

1. `arangodb`: A lightweight, minimalistic driver for interacting with ArangoDB. You can install it using the following command:

    ```
    npm install --save arangodb
    ```

    Once installed, you can use it to create a connection to your ArangoDB instance and perform various operations on the database. For example:

    ```javascript
    const arangodb = require('arangodb');
    const db = arangodb({
      url: 'http://localhost:8529',
      databaseName: 'mydb',
      auth: { username: 'myuser', password: 'mypassword' },
    });

    const collection = db.collection('mycollection');
    collection.save({ _key: 'mykey', myprop: 'myvalue' }).then(() => {
      console.log('Document saved!');"
}
```

AI vulnerabilities

The OWASP Top 10 for large language model vulnerabilities (LLMs) sheds further light on the risks posed by AI systems, such as susceptibility to prompt injections and errors in handling unexpected inputs, which can be exploited by cyber attackers.

AI-powered cyber security

While there's been plenty of coverage about the risks that have emerged from the widespread adoption of LLMs across industries, it's important to consider AI's role in enhancing cyber security measures. To repeat what we noted in our research, AI can assist in risk assessment, incident response, and ensuring compliance, besides analyzing the business impact of potential cyber threats.

There are clear benefits and some considerable risks attached to AI when it comes to cyber security. But, as with any new technology or solution, it's how you use it that matters.

Data leakage and information disclosure remain concerns

Data leakage remains a significant concern in 2023, with millions of records being exposed through data breaches, as we'll see especially with the final entry in our list for this quarter.

In particular, the finance sector experienced significant vulnerabilities because of database breaches. These breaches revealed sensitive information such as clients' personal details, business-related data, credit card numbers, and bank account information.

Indeed, according to data from Positive Technologies[1], data leakage accounted for 64% of the consequences of attacks faced by the finance sector.

Cloud security threats are on the rise

In 2023, cloud security challenges have been prominent due to increasing cloud adoption and complexity.

According to a report from Checkpoint[2], key challenges include misconfigurations and workloads moving to the cloud, making security and access management more complex. Data exfiltration is also a concern for organizations, exacerbated by cloud environments being accessible via the internet. Meanwhile, cloud security policy management and insecure APIs also present significant challenges.
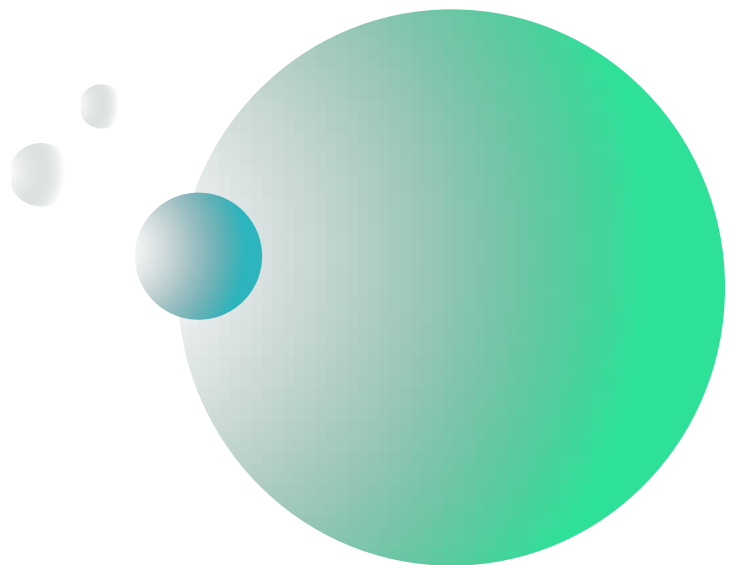
[1] Cyberthreats to the financial industry: interim results for 2023

[2] Top Cloud Security Challenges in 2023 - Check Point Software

Notable vulnerabilities of Q4 2023

CVE-2023-42115

Affected products:	All versions of Exim mail transfer agent (MTA) software
Product category:	Email security
Severity:	CVSS: 9.8	EPSS: N/A
Type:	Remote code execution
Impact:	N/A
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-42115 is a severe remote code execution vulnerability in Exim's SMTP service, caused by improper input validation. This flaw, with a high CVSS score of 9.8, allows remote attackers to execute arbitrary code by overflowing a buffer. Exim has addressed this issue in version 4.96.1, and updating to this version is crucial for mitigation. While there are no reports of active exploitation or public PoCs, Ubuntu has also issued security updates for this vulnerability.

CVE-2023-22515

Affected products:	Versions 8.0.0 through 8.5.1 of Confluence Server or Data Center
Product category:	Application security
Severity:	CVSS: 9.8	EPSS: 95.529%
Type:	Privilege escalation
Impact:	Integrity, confidentiality, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-22515 is a critical vulnerability in Confluence Data Center and Server, enabling attackers to create unauthorized administrator accounts and access these instances. Atlassian clarifies that Atlassian Cloud sites and atlassian.net domain Confluence instances are unaffected as they are Atlassian-hosted. With a CVSS score of 9.8, this vulnerability is highly severe. Atlassian has issued an advisory and security patches, and applying these patches is essential to reduce exploitation risks.

CVE-2023-20198

Affected products:	Web UI in Cisco devices running IOS XE
Product category:	Email security
Severity:	CVSS: 10 | EPSS: 89.074%
Type:	Privilege escalation
Impact:	Integrity, confidentiality, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-20198 is a severe vulnerability in Cisco IOS XE Software's web UI, enabling unauthenticated attackers to create a privileged account and potentially execute arbitrary commands. It has a maximum CVSS score of 10.0, reflecting its critical nature. Cisco has acknowledged active exploitation of this flaw and has released fixed versions and a Software Checker as part of their ongoing investigation. Organizations using affected Cisco products should urgently apply these security updates and mitigations.

CVE-2023-46604

Affected products:	Apache ActiveMQ & Apache ActiveMQ Legacy OpenWire
Product category:	Messaging systems
Severity:	CVSS: 9.8 | EPSS: 96.805%
Type:	Remote code execution
Impact:	Integrity, confidentiality, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-46604 is a critical vulnerability in Apache ActiveMQ, allowing remote attackers to execute arbitrary shell commands through insecure deserialization in the OpenWire protocol. This vulnerability impacts several versions of Apache ActiveMQ and its Legacy OpenWire Module. Apache addressed this issue with patches released on October 25, 2023. The vulnerability has been exploited in the wild, leading to incidents of HelloKitty Ransomware attacks, which encrypt files and demand ransom. Users of affected Apache ActiveMQ versions should urgently update to the provided patches to mitigate the risk.

CVE-2023-4966

Affected products:	Citrix NetScaler ADC and Gateway
Product category:	Network security / Application delivery controllers
Severity:	CVSS: 7.5 | EPSS: 91.792%
Type:	Sensitive information disclosure
Impact:	Confidentiality
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-4966 is a high-severity vulnerability in NetScaler ADC and NetScaler Gateway, with a CVSS score of 7.5. It leads to sensitive information disclosure when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server. This vulnerability is listed in CISA's Known Exploited Vulnerabilities Catalog, indicating its active exploitation. As it is currently under reanalysis, organizations using the affected software should stay alert for updated vulnerability summaries and adhere to guidance and requirements issued by CISA.

CVE-2023-46747

Affected products:	F5 BIG-IP version 17.1.0
	F5 BIG-IP version 16.1.0 – 16.1.4
	F5 BIG-IP version 15.1.0 – 15.1.10
	F5 BIG-IP version 14.1.0 – 14.1.5
	F5 BIG-IP version 13.1.0 – 13.1.5
Product category:	Network security / Application delivery controllers
Severity:	CVSS: 9.8 | EPSS: 96.55%
Type:	Remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

This flaw allows attackers with network access to bypass configuration utility authentication and execute arbitrary system commands. F5 has issued hotfixes to resolve this issue. To mitigate the risk of exploitation, it's essential to apply these patches promptly and ensure that the affected systems are not accessible from the public internet. Praetorian's researchers have chosen not to disclose specific details on triggering this vulnerability until an official patch is widely available.

CVE-2023-38547

Affected products:	Veeam ONE: 12 P20230314 (12.0.1.2591), 11a (11.0.1.1880), 11 (11.0.0.1379)
Product category:	IT infrastructure management software
Severity:	CVSS: 9.8 | EPSS: 0.24%
Type:	Remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

veeam

CVE-2023-38547 is a critical vulnerability in Veeam ONE, a monitoring platform, with a CVSS score of 9.9. It allows unauthenticated users to access information about the SQL server connection used by Veeam ONE for its configuration database. This vulnerability could lead to remote code execution (RCE) on the SQL server hosting the Veeam ONE configuration database. Veeam has responded by releasing hotfixes to rectify this issue. To reduce the risk of exploitation, it's vital for users to promptly apply these patches.

CVE-2023-36553

Affected products:	FortiSIEM releases 4.7 through 5.4.
Product category:	Security information and event management (SIEM)
Severity:	CVSS: 9.8 | EPSS: 3.075%
Type:	Command injection
Impact:	Confidentiality, integrity, availability
PoC:	No
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

FORTINET

CVE-2023-36553 is a vulnerability in Fortinet FortiSIEM versions ranging from 4.7.2 to 5.4.0. It involves improper neutralization of special elements used in an OS command ('OS command injection'), allowing an attacker to execute unauthorized code or commands through crafted API requests. This vulnerability affects multiple versions of FortiSIEM, including 5.3.0 to 5.3.3, 5.2.5 to 5.2.8, 5.2.1 to 5.2.2, 5.1.0 to 5.1.3, 5.0.0 to 5.0.1, 4.10.0, 4.9.0, and 4.7.2. The exploitation of this vulnerability could lead to significant security risks, including unauthorized access and control over the affected systems.

CVE-2023-6345

Affected products:	Google Chrome up to version CVE-2023-6345 (Windows), 119.0.6045.199 (MaxOS, Linux)
Product category:	Internet browser
Severity:	CVSS: 9.8 | EPSS: 3.908%
Type:	Integer overflow
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-6345 is an integer overflow vulnerability in Skia within Google Chrome, affecting versions prior to 119.0.6045.199. This vulnerability allowed a remote attacker, who had already compromised the renderer process, to potentially perform a sandbox escape using a malicious file. Classified with a high security severity by Chromium, this vulnerability posed a significant risk, as it could enable attackers to escape the browser's security sandbox and execute arbitrary code on the host system.

CVE-2023-49105

Affected products:	OwnCloud, ownCloud/core before 10.13.1 (Earliest affected version: 10.6.0)
Product category:	File sharing software
Severity:	CVSS: 9.8 | EPSS: 20.581%
Type:	Privilege escalation, remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-49105 is a vulnerability discovered in ownCloud (owncloud/core) versions before 10.13.1, starting from version 10.6.0. This issue allows an attacker to access, modify, or delete any file without authentication, provided they know the username of a victim who does not have a signing-key configured. The vulnerability arises because pre-signed URLs can be accepted even when no signing-key is configured for the file owner. This security flaw poses a significant risk as it bypasses the authentication mechanism, potentially leading to unauthorized data access or manipulation. Users of affected ownCloud versions are advised to update to version 10.13.1 or later to mitigate this vulnerability.

CVE-2023-50164

Affected products:	Apache Struts 2.0.0 through 2.5.32 Apache Struts 6.0.0 through 6.3.0.1
Product category:	Application framework / software development framework
Severity:	CVSS: 9.8 | EPSS: 9.799%
Type:	Path traversal remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-50164 is a vulnerability in Apache Struts, where an attacker can manipulate file upload parameters to enable path traversal. Under certain conditions, this can lead to the uploading of a malicious file, which can be used to perform Remote Code Execution (RCE). To address this issue, users are recommended to upgrade to Struts versions 2.5.33, 6.3.0.2, or later. This vulnerability highlights the importance of secure file upload handling and the need for regular updates to web application frameworks to mitigate such risks.

MongoDB

While not a CVE, this warrants a mention in our report due to the impact of this breach.

MongoDB experienced a significant security incident involving unauthorized access to its corporate systems, discovered on December 13, 2023. This breach led to the exposure of customer account metadata and contact details but did not compromise data stored in MongoDB Atlas.

MongoDB's response included activating their incident response plan and recommending enhanced security measures for users, such as phishing-resistant multi-factor authentication and regular password changes. The incident highlights the increasing complexity of the attack surface and the importance of swift, effective incident response and risk-based vulnerability management.

Summary

As we enter 2024, the overarching narrative is clear. The attack surface, already growing over the past few years, has not slowed its expansion, and shows no signs of doing so. In the face of this, organizations can ill-afford to work with siloed data, solutions and teams, or rely on vulnerability management workflows no longer fit for the widening threat landscape.

Exposure management presents a way forward, bringing disparate data under one roof, and allowing teams to manage and mitigate risk from one place.

VULCAN.

Exposure management
Secure the entire attack surface in one operational view

RBVM

Prioritize the most critical vulnerability risk.

- **v** Business-context
- **v** Risk prioritization
- **v** Remediation orchestration

ASPM

Secure cloud-native application assets.

- **v** Coverage management
- **v** Root-cause analysis
- **v** Correlation and triage
- **v** Dev/security collaboration

CAASM

Discover assets within the organizer's digital infrastructure.

- **v** Asset correlation
- **v** Visibility gaps analysis
- **v** Continuous compliance

Cloud VM

Find and fix security gaps in the cloud infrastructure.

- **v** Code-to-cloud remediation
- **v** Cloud risk management
- **v** Multi-cloud consolidation

As technologies and the associated cyber risk evolve, it's integral that teams take action to unify their vulnerability data, and take meaningful action against the risk that matters most.

About Vulcan Cyber

Vulcan Cyber enables security teams to effectively manage and reduce vulnerability risk across IT and cloud-native surfaces. The platform consolidates vulnerability scan and threat intelligence data from all attack surfaces and provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a 2019 Gartner Cool Vendor, a 2020 RSA Conference Innovation Sandbox finalist and as a Leader in the Q3 2023 Vulnerability Risk Management Forrester Wave. Prominent security teams, such as those at Mandiant, Deloitte, and Snowflake, trust Vulcan Cyber to help them own their risk.

Start owning your risk

TRY VULCAN FREE

About Voyager18

The Vulcan Cyber research team, also known as Voyager18, is a team of cyber experts working to leverage machine learning and cyber research to ensure Vulcan Cyber remains a cyber security leader. The team's main objective is to research the latest cyber risk trends, including new attack types and remediations. Most recently, they discovered AI package hallucination in OpenAI's ChatGPT. Voyager18 is also responsible for bringing innovation to the Vulcan Cyber platform so that our customers get improved and customized cyber risk management capabilities. Alongside the new attack path graph feature, the team mapped out the MITRE ATT&CK framework to relevant CVEs, providing granular insights into the most critical vulnerabilities.

Stay up to date with the latest research here >>