VULCAN.

VOYAGER18

Q1 2024 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 first quarter of 2024. Updated through March 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 2023, 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 Q1 2024

In the past three months, the cyber security landscape has been dynamic, with a significant number of vulnerabilities and exploits emerging. Over 7,000 CVEs[1] were published during this period, highlighting the ongoing challenges in securing digital systems. These vulnerabilities span various categories, from authentication bypass to misconfigurations, emphasizing the diverse nature of cyber threats faced by organizations and individuals.

The need for proactive patching and robust security measures is underscored by the continuous evolution of cyber risks, making it imperative for stakeholders to stay vigilant and prioritize cyber security efforts in the face of escalating threats.

Here are just some of the trends we identified:

AI manipulation: The threat continues

Continuing AI security threats pose significant risks in the cyber security landscape. One notable concern is the emergence of backdoor threats, exemplified by the Hugging Face example highlighted below. These threats involve malicious actors exploiting vulnerabilities in AI systems to gain unauthorized access or manipulate data, potentially leading to severe consequences such as data breaches and compromised system integrity.

The sophistication of AI technologies can inadvertently create new avenues for cyber attacks, emphasizing the critical need for robust security measures and proactive risk mitigation strategies to safeguard against evolving AI-related threats.

[1] CVE details from Security Scorecard

CISA targeted in Ivanti exploit

The recent breach of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) due to hackers exploiting vulnerabilities in Ivanti products (below) underscores the critical importance of effective vulnerability management for government agencies.

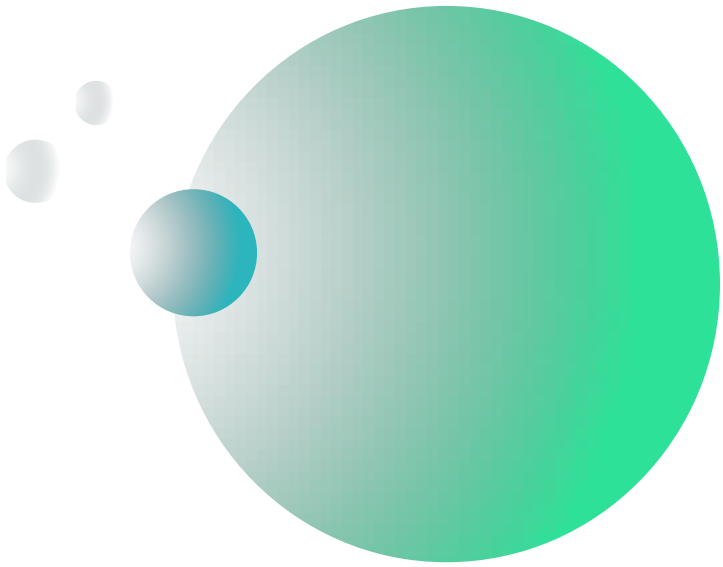
The breach serves as a stark reminder of the significance of timely patching, proactive vulnerability identification, and robust cyber security protocols in safeguarding government systems against sophisticated cyber threats.

Compliance in focus

NIST 2.0, released this quarter, has garnered significant attention in the cyber security community. This updated framework aims to enhance global cyber security risk management practices, building on the original document.

Alongside NIST 2.0, compliance standards like DORA and NIS2 are also gaining prominence, with DORA focusing on ensuring the integrity and availability of the financial sector and NIS2 strengthening cyber security within the EU across various sectors.

These frameworks collectively underscore the growing emphasis on robust cyber security measures and compliance standards to address evolving cyber threats effectively.



Notable vulnerabilities of Q1 2024

CVE-2023-7102

Affected products:	Barracuda ESG Appliance, from 5.1.3.001 through 9.2.1.001
Product category:	Email/network security
Severity:	CVSS: 9.8 | EPSS: 8.2%
Type:	Arbitrary 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-2023-7102 is a zero-day vulnerability in Barracuda Networks Inc.'s Email Security Gateway appliances, allowing arbitrary code execution through a flaw in the Spreadsheet::ParseExcel library. Exploited by UNC4841, it facilitated the deployment of SEASPY and SALTWATER implants via malicious Excel email attachments. Barracuda issued a security update on December 21, 2023, to address the issue and protect affected devices.

CVE-2023-46805

Affected products:	Ivanti Connect Secure or Ivanti Policy Secure
Product category:	IT software
Severity:	CVSS: 8.2 | EPSS: 92.4%
Type:	Authentication bypass
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

The exploitation of CVE-2023-46805 in Ivanti Connect Secure and Ivanti Policy Secure gateways has led to significant cyber security concerns, particularly for CISA, who experienced their own breach through this vulnerability. Threat actors have been exploiting CVE-2023-46805 to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges. CISA has issued emergency directives to address these vulnerabilities and mitigate the risks posed by the exploitation of Ivanti devices.

CVE-2024-21887

Affected products:	Ivanti Connect Secure or Ivanti Policy Secure
Product category:	IT software
Severity:	CVSS: 9.1 | EPSS: 95.7%
Type:	Command injection
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

The exploitation of CVE-2024-21887 in Ivanti gateways allows attackers to execute unauthorized commands, leading to data breaches and unauthorized access. Ivanti is actively working on patches and interim solutions to mitigate this vulnerability.

CVE-2023-6549

Affected products:	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35 NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15 NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21 NetScaler ADC 13.1-FIPS before 13.1-37.176 NetScaler ADC 12.1-FIPS before 12.1-55.302 NetScaler ADC 12.1-NDcPP before 12.1-55.302
Product category:	Network access
Severity:	CVSS: 7.5 | EPSS: 1.9%
Type:	Denial-of-service
Impact:	Availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-6549 is a critical vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway products, leading to a denial-of-Service attack. To address this issue, users should promptly update their affected appliances with the latest security patches released by Citrix. Immediate action is crucial to prevent exploitation of this vulnerability and safeguard the integrity of the systems.

CVE-2023-22527

Affected products:	Atlassian's Confluence Server and Data Center
Product category:	Software
Severity:	CVSS: 9.8 | EPSS: 8.2%
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

CVE-2023-22527 is a critical vulnerability in Atlassian Confluence Data Center and Server, classified as a template injection flaw that allows remote code execution without authentication. This vulnerability poses a severe risk to organizations by enabling attackers to execute arbitrary code on the Confluence server, potentially leading to unauthorized access and control over affected systems.

CVE-2024-0204

Affected products:	Fortra GoAnywhere MFT 6.x from 6.0.1 Fortra GoAnywhere MFT 7.4.0 and earlier
Product category:	Unified communications software
Severity:	CVSS: 9.8 | EPSS: 0.1%
Type:	Path traversal weakness
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-0204 is a critical vulnerability in Fortra's GoAnywhere MFT before version 7.4.1, allowing unauthorized admin account creation. Fortra has released patches to address this issue, and users are advised to update to the latest version for security.

CVE-2024-20253

Affected products:	Cisco Unified CM, IM, IM&P, CM SME, UCCX, Unity Connection, VVB
Product category:	Unified communications software
Severity:	CVSS: 10 | EPSS: 12.3%
Type:	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-2024-20253 is a critical remote code execution vulnerability affecting various Cisco Unified Communications and Contact Center Solutions products. The vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the web services user. Cisco has released patches to address the issue, and immediate patching or setting up access control lists (ACLs) on intermediary devices is recommended.

CVE-2024-21762

Affected products:	Fortinet FortiOS versions 7.4.0 through 7.4.2 7.2.0 through 7.2.6, 7.0.0 through 7.0.13 6.4.0 through 6.4.14, 6.2.0 through 6.2.15 6.0.0 through 6.0.17 FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7
Product category:	Operating system
Severity:	CVSS: 9.8 | EPSS: 1.2%
Type:	Out-of-bound write leading to 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

CVE-2024-21762 is a critical vulnerability in Fortinet FortiOS and FortiProxy versions, allowing attackers to execute unauthorized code or commands through specially crafted requests. This vulnerability has a base score of 9.8, indicating its severity. Organizations using affected versions are advised to apply patches promptly to mitigate the risk of exploitation.

CVE-2024-21413

Affected products:	Microsoft Office 2016 (64-bit editions) Microsoft Office 2016 (32-bit editions) Microsoft Office 2019 (64-bit editions) Microsoft Office 2019 (32-bit editions) Microsoft Office LTSC 2021 (32-bit editions) Microsoft Office LTSC 2021 (64-bit editions) Microsoft 365 Apps for Enterprise (64-bit Systems) Microsoft 365 Apps for Enterprise (32-bit Systems)
Product category:	Email provider
Severity:	CVSS: 9.8 | EPSS: 37.3%
Type:	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-2024-21413 is a critical zero-day vulnerability in Microsoft Outlook that allows remote code execution through specific hyperlinks. Microsoft has released security updates to address this issue, and users should update promptly to prevent exploitation.

CVE-2024-27198

Affected products:	All JetBrains TeamCity On-Premises versions through 2023.11.3
Product category:	CI/CD
Severity:	CVSS: 9.8 | EPSS: 7%
Type:	Authentication bypass/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

CVE-2024-27198 is a critical vulnerability affecting JetBrains TeamCity, allowing authentication bypass and potentially enabling remote code execution. This vulnerability poses a significant risk with a CVSS score of 9.8. It impacts versions of TeamCity before 2023.11.4. Urgent action is required to update affected instances to the patched version to mitigate this security threat. Additionally, applying security hardening configurations is recommended to limit the impact of potential remote code execution attacks.

CVE-2024-21400

Affected products:	Azure Kubernetes Service Confidential Containers
Product category:	Container
Severity:	CVSS: 9 | EPSS: 37.6%
Type:	Elevation of privilege
Impact:	Confidentiality, integrity, availability
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-21400 is a critical vulnerability addressed in the March 2024 Patch Tuesday updates for Windows and SharePoint. This security fix is part of Microsoft's efforts to enhance the security of these systems by addressing potential vulnerabilities.

Hugging Face backdoor

Affected products:	Hugging face
Product category:	Software application
Severity:	N/A
Type:	AI manipulation
Impact:	N/A
PoC:	Yes
Exploit in the wild:	N/A
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	No

A backdoor threat targeting Hugging Face, a key platform for AI models and datasets, has raised alarms in the AI community. The vulnerability affects the Safetensors conversion service, essential for the security of shared machine learning models. By submitting compromised pull requests, attackers can introduce backdoors into models, risking unauthorized data access and model tampering.

Hugging Face has responded by strengthening its security measures. Yet, this incident highlights the ongoing challenge of supply chain vulnerabilities in AI, underscoring the importance of stringent security practices, thorough code reviews, and a vigilant community culture.

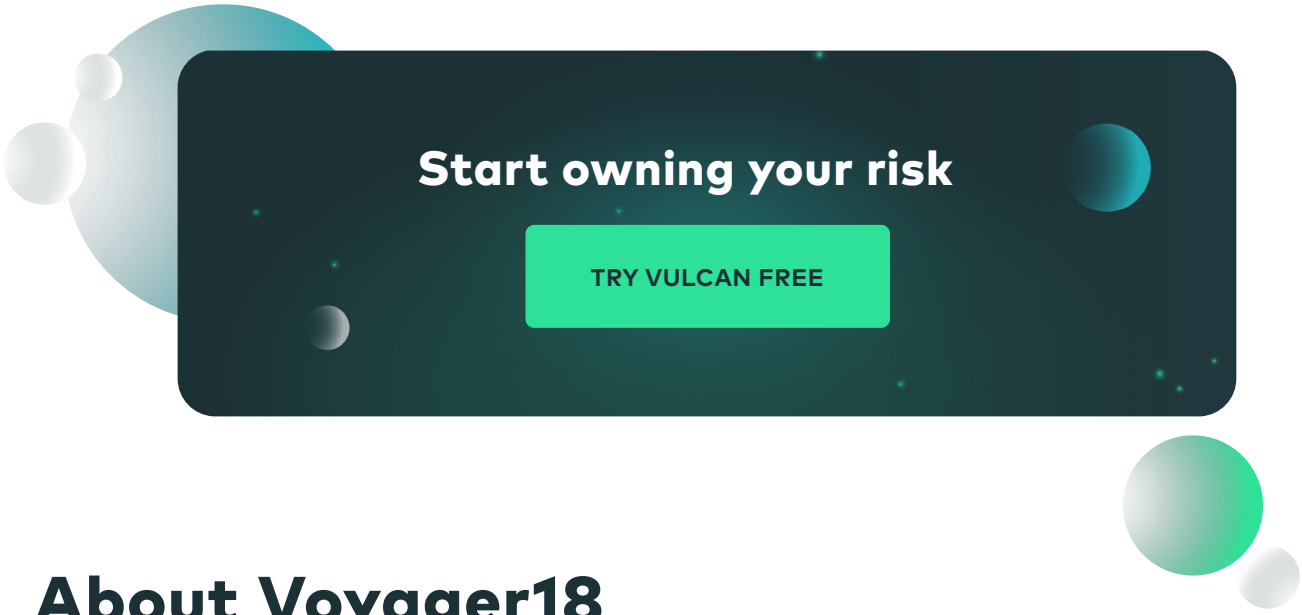
As AI technology advances, platforms like Hugging Face must continuously prioritize security to protect the integrity of machine learning models and datasets, requiring a collaborative approach among developers, security experts, and users to mitigate risks effectively.

Summary

The first quarter of 2024 saw a dynamic cyber security environment, with a high number of vulnerabilities and the continuing trends of AI-related threats The emphasis on adherence to frameworks like NIST 2.0, DORA, and NIS2 reflects a heightened focus on cyber security and. compliance to counteract these threats. Urgent action is required to address the significant vulnerabilities identified in Q1 and beyond, ensuring system integrity and resilience.

About Vulcan Cyber

Vulcan Cyber ExposureOS is the one platform for managing exposure risk across IT and cloud-native surfaces. At its core, ExposureOS aggregates and correlates security findings from your infrastructure, code, application, and cloud environments into the exposure data lake. The platfrom then 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 2023 Forrester Wave Leader and a 2020 RSA Conference Innovation Sandbox finalist. Prominent security teams,



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 >>