VULCAN. VOYAGER18

Q3 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 third quarter of 2023. Updated through September 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 and Q2, 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.

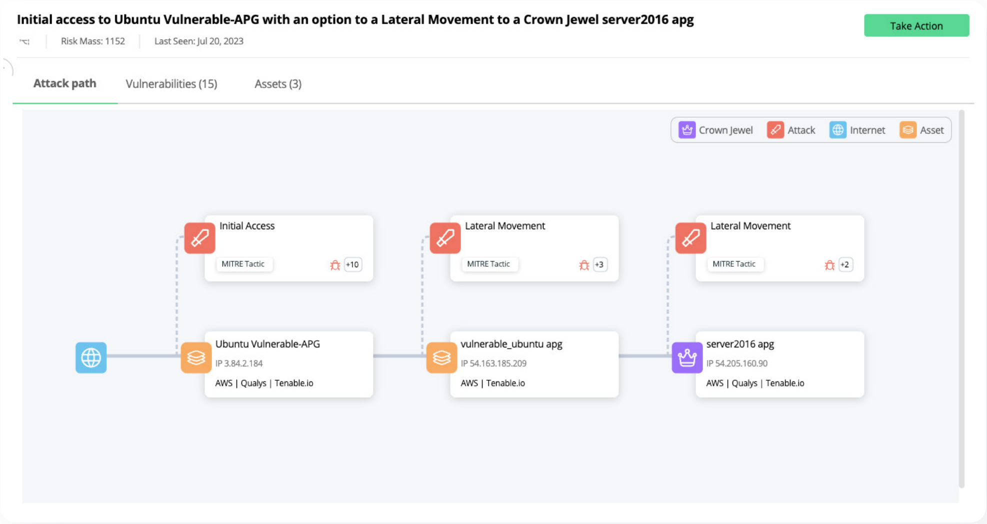
The story of Q3 2023

This quarter has been marked by the steady occurrence of critical vulnerabilities in widely used products and services like MacOS, Microsoft Windows, OpensSSH and more. Remote code execution has been a repeat concern, and security teams have had to explore urgent mitigation actions to counter the threats.

The introduction of attack path analysis

Attack path analysis is the charting of the sequential actions an attacker may undertake to exploit a vulnerability and breach a system or network. It serves as a vital methodology to help security teams comprehend the potential ramifications of a vulnerability, thus aiding in prioritizing their remediation strategies.

This approach usually encapsulates details pertaining to the exploited vulnerability, the initial point of intrusion utilized by the attacker, the variety of tools and techniques employed for lateral movements within the network, and the final objective of the attack. The new Vulcan Cyber Attack Path Graphs feature provides visual representations of this analysis.



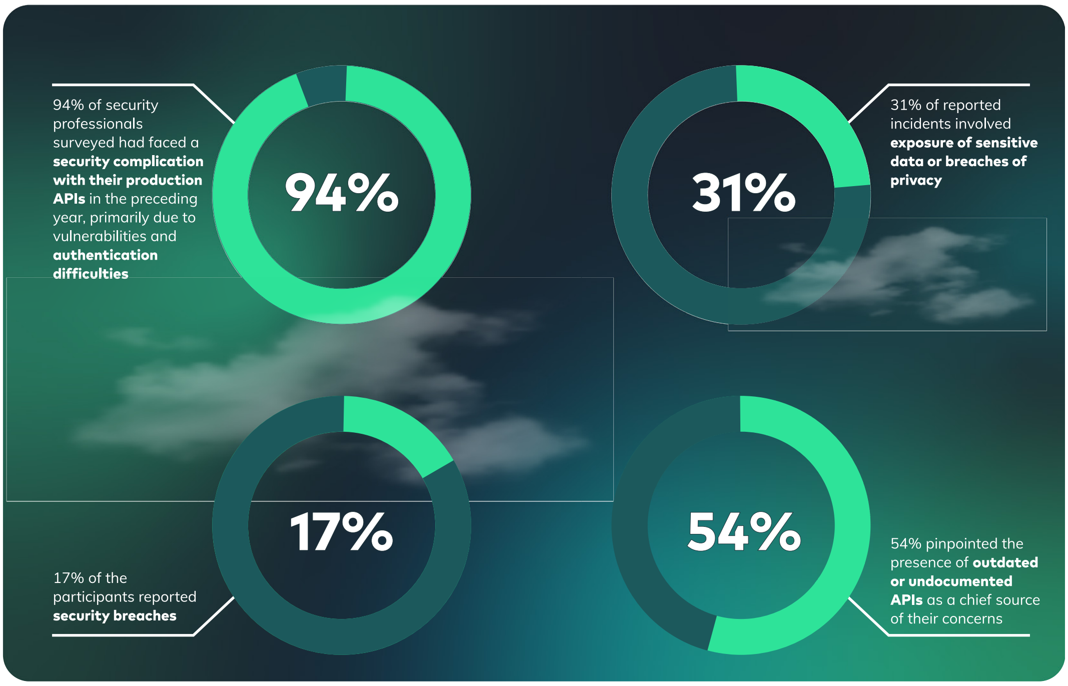
Initial access to Ubuntu Vulnerable-APG with an option to a Lateral Movement to a Crown Jewel server2016 apg

Risk Mass: 1152 | Last Seen: Jul 20, 2023

By delineating these stages graphically, security teams are equipped to pinpoint possible shortcomings in their protective measures, facilitating the formulation and implementation of strategies to lessen the likelihood of successful exploitations.

The challenges of API security

API security continues to be a prominent issue in Q3 2023. A recent study[1] revealed:



94% of security professionals surveyed had faced a **security complication with their production APIs** in the preceding year, primarily due to vulnerabilities and **authentication difficulties**

31% of reported incidents involved **exposure of sensitive data or breaches of privacy**

17% of the participants reported **security breaches**

54% pinpointed the presence of **outdated or undocumented APIs** as a chief source of their concerns

The 2023 edition of the OWASP API Security Top 10 crystallizes our understanding of the potential risks associated with APIs. It outlines critical areas of concern, such as compromised object-level authentication, fragile authentication procedures, flawed object property-level authorization, unchecked resource usage, malfunctioning function-level authorization, inadequate logging and surveillance mechanisms, subpar attack defenses, weak operational security measures, unsatisfactory security configurations, and insufficient measures to safeguard data.

In light of these findings, it's evident that API security remains a paramount issue for organizations worldwide. It is incumbent upon these entities to foster a more secure digital environment by pinpointing and rectifying vulnerabilities, reinforcing authentication and authorization protocols, and enhancing logging and monitoring frameworks to secure their APIs effectively.

[1] https://salt.security/api-security-trends

Notable vulnerabilities of Q3 2023

CVE-2023-37450

Affected products:	Webkit Engine in iOS versions prior to 16.5.1(a) Webkit Engine in iPadOS versions prior to 16.5.1(a) Webkit Engine in macOS versions prior to Ventura 13.4.1(a) Webkit Engine in Safari versions prior to 16.5.2
Product category:	Operating system
Severity:	CVSS: 8.8 | EPSS: 0.095%
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

The WebKit browser engine has a recognized vulnerability, marked as CVE-2023-37450, which poses a significant risk to Apple devices. This security breach could grant a hacker the ability to launch arbitrary code while handling web material. To counter this, enhancements in security protocols were established, resulting in the rectification of the issue in various software versions, including iOS 16.6 and iPadOS 16.6, Safari 16.5.2, tvOS 16.6, macOS Ventura 13.5, and watchOS 9.6. Responding to the ongoing active exploitation of this vulnerability, Apple swiftly launched an emergency correction to curb the vulnerability and protect affected platforms.

CVE-2023-38408

Affected products:	PKCS#11 feature in SSH-agent in OpenSSH before 9.3p2
Product category:	Third-party software
Severity:	CVSS: 9.8 | EPSS: 3.651%
Type:	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

The vulnerability tagged as CVE-2023-38408 has been identified within the PKCS11 functionality of the ssh-agent in OpenSSH. This flaw stems from a search path that isn't sufficiently secure, paving the way for potential remote code execution.

To rectify this security loophole, users are urged to upgrade to OpenSSH version 9.3p2 or a more recent version, which contains a fix addressing this particular concern. Performing this update will fortify the ssh-agent's PKCS11 feature with a more robust search path, thereby reducing the likelihood of remote code execution incidents.

CVE-2023-3519

Affected products:	Citrix NetScaler
Product category:	Third-party software
Severity:	CVSS: 9.8 | EPSS: 88.985%
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

The CVE-2023-3519 vulnerability in Citrix ADC and Citrix Gateway allows remote code execution by attackers. First identified as a zero-day in mid-July 2023, it was actively exploited to upload malicious TGZ files on the ADC. Citrix has issued a security bulletin and recommends applying the necessary patches to prevent further exploitation.

CVE-2023-20214

Affected products:	SD-WAN vManage 20.6.3.4, 20.6.4.2, 20.6.5.5, 20.9.3.2, 20.10.1.2, and 20.11.1.2. SD-WAN vManage versions 20.7 and 20.8 are advised to migrate to patched version
Product category:	Virtual architecture
Severity:	CVSS: 9.1 | EPSS: 0.102%
Type:	Authentication bypass
Impact:	Confidentiality, integrity, availability
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

The CVE-2023-20214 vulnerability detected in Cisco's SD-WAN vManage software can potentially allow unauthorized access to the REST API, enabling unauthenticated users to undertake unauthorized activities. Cisco has issued a security advisory with patches to address this significant flaw.

It's highly advisable for users of this software to reference the security advisory swiftly and apply the necessary patches to prevent potential exploitation. In addition, users should adhere to best security practices, such as implementing secure authentication mechanisms and limiting access to critical systems and data, to bolster overall security.

CVE-2023-35385

Affected products:	Windows 10, 11 and Server 2008-2022 platforms
Product category:	Operating system
Severity:	CVSS: 9.8 | EPSS: 0.8%
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

The CVE-2023-35385 vulnerability found in Microsoft Message Queuing (MSMQ) could potentially enable an attacker to remotely execute code. Microsoft has responded to this vulnerability with a security update that offers necessary patches to lessen the risk of exploitation.

Users utilizing Microsoft Message Queuing should promptly consult the Microsoft security update and implement the recommended patches to rectify this vulnerability. Moreover, it is advised to adhere to security best practices, which include establishing robust authentication procedures and limiting access to confidential systems and data, to further safeguard against potential threats.

CVE-2023-36910

Affected products:	Windows 10, 11 and Server 2008-2022 platforms
Product category:	Operating system
Severity:	CVSS: 9.8 | EPSS: 0.8%
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

Similar to the above, CVE-2023-36910 exists in Microsoft Message Queuing (MSMQ), presenting a risk where an attacker might execute code remotely. Microsoft has released a security update to address this issue, urging users to apply the provided patches to minimize the exploitation risk.

If you are utilizing Microsoft Message Queuing, it is advisable to review the Microsoft security update and promptly apply the necessary patches to mitigate the vulnerability.

CVE-2023-36911

Affected products:	Windows 10, 11 and Server 2008-2022 platforms
Product category:	Operating system
Severity:	CVSS: 9.8 | EPSS 0.8%
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

The CVE-2023-36911 vulnerability, akin to the previously mentioned Microsoft vulnerabilities, resides in the MSMQ and has the potential to let an attacker execute code remotely. Microsoft has released a security update to counter this vulnerability, advising users to install the relevant patches to reduce the chances of exploitation.

CVE-2023-39143

Affected products:	PaperCut NG and PaperCut MF versions prior to v22.1.3
Product category:	Third-party software
Severity:	CVSS: 9.8 | EPSS: 89.139%
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

The CVE-2023-39143 vulnerability, a critical issue discovered in the PaperCut Print Management Server, could potentially enable unauthorized attackers to read, delete, and upload arbitrary files on compromised systems, thereby facilitating remote code execution. This vulnerability, rooted in path traversal and file upload issues, could potentially allow attackers to upload malicious files onto the PaperCut MF/NG application.

In response to this, PaperCut has rectified the vulnerability in its 22.1.3 version. To minimize the risk of exploitation, it's recommended to upgrade to this latest version promptly. Users of the PaperCut Print Management Server should consult the PaperCut security advisory and undertake the necessary patch implementations to neutralize the threat.

CVE-2023-40477

Affected products:	WinRAR before 6.23
Product category:	Third-party software
Severity:	CVSS: 8.8 | EPSS: N/A
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

The CVE-2023-40477 vulnerability exists in WinRAR, a popular file archiver utility for Windows. This vulnerability stems from a buffer overflow that might happen during the processing of recovery volume names in the outdated RAR 3.0 format, potentially allowing an attacker to execute code remotely.

RARLAB has addressed this issue through a security update, urging users to upgrade WinRAR to the most recent version to lessen the likelihood of exploitation. If you are utilizing WinRAR, it's crucial to regularly check for updates and implement the necessary patches to rectify the vulnerability. Moreover, it is advised to adhere to security best practices, which include avoiding the extraction of files from sources that are unknown or not trusted, to enhance your protection against potential threats.

CVE-2023-2868

Affected products:	Barracuda Email Security Gateway Appliances versions 5.1.3.001-9.2.0.006
Product category:	Email security
Severity:	CVSS: 9.8 | EPSS: 2.4%
Type:	Remote 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 CVE-2023-2868 vulnerability in Barracuda Email Security Gateway (ESG) appliances could potentially enable remote command injections by attackers, originating from inadequate input validation for user-supplied .tar files. This flaw has been exploited by threat actors since at least October 2022.

Barracuda Networks has launched a security patch to counter this vulnerability, encouraging users to update to the newest version to reduce exploitation risks. Moreover, the FBI and Barracuda Networks advise the immediate replacement of ESG devices to bolster network security. Users of Barracuda ESG should vigilantly check for compromise indicators and promptly apply patches or replace affected devices to address the issue.

CVE-2023-34039

Affected products:	Aria Operations for Networks versions 6.2 / 6.3 / 6.4 / 6.5.1 / 6.6 / 6.7 / 6.8 / 6.9 / 6.10
Product category:	IT operations
Severity:	CVSS: 9.8 | EPSS: 0.905%
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

VMware Aria Operations™

The CVE-2023-34039 vulnerability, identified in VMware Aria Operations for Networks (previously vRealize Network Insight), could potentially permit an attacker to circumvent authentication measures and execute commands with root privileges. This issue arises from the absence of unique cryptographic key generation, facilitating attackers to use a static SSH key to gain unauthorized access to the system.

VMware has been informed of this vulnerability through responsible disclosure, and has issued a security patch to rectify the problem. Users are urged to update to the latest version of VMware Aria Operations for Networks to minimize the risk of exploitation. Those utilizing this platform should remain vigilant, frequently check for updates, and install the necessary patches to alleviate the vulnerability.

Summary

Q3 2023 has shown the increasing reliance of organizations on third-party software and APIs. While there are clear benefits to this, they should be conscious of the accompanying security considerations. New technologies and tools will broaden the attack landscape and result in greater numbers of vulnerabilities. Smart and contextual prioritization is necessary to ensure that security teams are not overloaded with cyber risk data and noise preventing them from achieving better cyber hygiene.

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 >>