VULCAN.

VOYAGER18

Q2 2023 Vulnerability Watch

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

Table of contents

Introduction

This report spotlights **notable vulnerabilities** discovered during the second quarter of 2023. Updated as of June 26th, 2023, it outlines the potential impact of these vulnerabilities and offers practical insights to help organizations strengthen their vulnerability risk management efforts.

In addition to providing comprehensive technical details about CVEs, the report goes beyond their severity rating in the Common Vulnerability Scoring System (CVSS) by including information about their Exploitability Score (EPSS) and presence in the catalog maintained by the Cybersecurity and Infrastructure Security Agency (CISA), among other relevant data.

The story of Q2 2023

This quarter has been punctuated by zero-day threats and a spread of vulnerability risk across a variety of products and technologies, including Google Chrome and Apache Superset. Nonetheless, it's the last item on this list - "AI package hallucination" - that has intrigued us the most.

The challenge of AI

LLM risks are naturally a major concern, and have been a hot topic since the groundbreaking release of ChatGPT in November 2022. Our research demonstrates that we will only encounter more avenues of opportunity for attackers in this space. As we show below, and in greater detail in our blog post, ChatGPT's hallucinatory tendencies give attackers a unique opportunity to take advantage of unsuspecting users.

We're heading into uncharted waters. Generative AI is developing at an unprecedented pace, and while it makes workflows easier for many of us, we need to prepare for threat actors to reap the benefits as well.

CVSS 4.0 is here (almost)

CVSS v4.0, a new version of the Common Vulnerability Scoring System, offers enhanced granularity, support for multiple exploit vectors, and a new environmental metrics group.

CVSS v3.1	VS.	CVSS v4.0
CVSS 3.1 is the current version of the Common Vulnerability Scoring System framework, widely used for assessing and prioritizing software vulnerabilities.		**CVSS 4.0 builds upon the foundation of CVSS 3.1 and introduces additional parameters like environmental factors, threat metrics, and further customization.**
One per vulnerability	CVSS SCORE	Multiple per vulnerability
Exploitability metrics (4)	BASE METRIC GROUP	Exploitability metrics (5) New: "Attack requirements"
Impact metrics - system (3)		Impact metrics - system (3) subsequential (3)
Scope		N/A
User interaction (2)		User interaction (3) New: "Passive"
0-10	SCORING RANGE	0-10
Temporal (3)	THREAT METRIC GROUP	Threat (1) New: "Exploit maturity"
Modified case metrics (8)	ENVIRONMENTL METRIC GROUP	Modified case metrics (11)
Environmental		Environmental, supplemental New: "Supplemental"
Limited customization	CUSTOMIZATION	Higher customization

Sources: FIRST: www.first.org/cvss/v4-0/ | **Official CVSS 4.0 documentation and guidelines** www.first.org/cvss/v4-0/cvss-v40-specification.pdf

Developed as a response to criticisms of the previous version's complexity and inflexibility, v4.0 provides simpler, more flexible, and more accurate scoring. It aims to provide a more realistic representation of risks, thereby helping organizations to better prioritize vulnerabilities and allocate remediation resources. This significant revision is expected to greatly impact how security practitioners assess and prioritize vulnerabilities. You can read our full write-up of CVSS v4.0 here.

Notable vulnerabilities of Q2 2023

CVE-2023-32784

Affected products:	KeePass 2.x prior to 2.54
Product category:	Password manager
Severity:	CVSS: 7.5 | EPSS: 0.065%
Type:	Master password retrieval (unauthorized access), memory corruption
Impact:	Confidentiality
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-32784 is a memory corruption vulnerability in KeePass 2.x before 2.54. This vulnerability can be exploited by an attacker to recover the cleartext master password from a memory dump. The first character of the master password cannot be recovered. To mitigate the risk of exploitation, users should upgrade to KeePass 2.54 or later.

CVE-2023-32243

Affected products:	Essential Addons plugin prior to version 5.7.2
Product category:	Third party software
Severity:	CVSS: 9.8 | EPSS: 0.85%
Type:	Privilege escalation
Impact:	Attacker can gain admin access to a WordPress site
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-32243 is a privilege escalation vulnerability in Essential Addons for Elementor, a WordPress plugin. An attacker can exploit this vulnerability to gain administrator privileges on a vulnerable WordPress site. To mitigate the risk, users should update to Essential Addons for Elementor version 5.7.2 or later. If updating is not possible, users should use a strong password for the administrator account and enable two-factor authentication.

CVE-2023-1671

Affected products:	Sophos Web Appliance prior to version 4.3.10.4
Product category:	Third party software
Severity:	CVSS: 9.8 | EPSS: 18.82%
Type:	Command injection, execution of arbitrary code
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-1671 is a critical vulnerability in Sophos Web Appliance prior to version 4.3.10.4. It allows an attacker to execute arbitrary code on the remote system by exploiting a pre-authentication command injection vulnerability in the warn-proceed handler. This vulnerability can be exploited by sending a specially crafted HTTP request to the vulnerable system. The attacker can then use this vulnerability to install malware, steal data, or disrupt operations.

CVE-2023-27524

Affected products:	Apache Superset versions prior to 2.0.1
Product category:	Web application
Severity:	CVSS: 9.8 | EPSS: 74.33%
Type:	Session validation attacks, access and authentication to unauthorized resources
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-27524 is a critical vulnerability in Apache Superset versions up to and including 2.0.1. It allows an attacker to authenticate and access unauthorized resources by exploiting an insecure default configuration. The vulnerability occurs because Apache Superset is configured with a default SECRET_KEY that is known to attackers. This allows attackers to forge a session cookie with a user_id value of 1, which is usually the admin user. Once the attacker has authenticated as an admin user, they can access any data or functionality in Apache Superset.

CVE-2023-29199

Affected products:	VM2 JS library prior to 3.9.15
Product category:	Web application
Severity:	CVSS: 10 | EPSS: 0.60%
Type:	Bypass sandbox protections, remote code execution (host context)
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-29199 is a critical vulnerability in the source code transformer (exception sanitization logic) of VM2, a sandbox for running untrusted code, for versions up to 3.9.15. It allows attackers to bypass the handleException() function and leak unsanitized host exceptions, which can be used to escape the sandbox and run arbitrary code in the host context. Essentially, this means that a threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. The vulnerability was patched in version 3.9.16 of vm2.

CVE-2023-30547

Affected products:	VM2 JS library prior to 3.9.16
Product category:	Web application
Severity:	CVSS: 10 | EPSS: 0.12%
Type:	Bypass sandbox protections, remote code execution (host context)
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-30547 is a critical severity vulnerability that affects the VM2 package up to version 3.9.16. VM2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. The vulnerability allows attackers to raise an unsanitized host exception inside handleException(), which can be used to escape the sandbox and run arbitrary code in the host context. This means a threat actor could bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. There are no known workarounds for this vulnerability, and users are advised to upgrade to VM2 version 3.9.17, where the issue was patched.

CVE-2023-2033

Affected products:	V8 JavaScript engine in Google Chrome versions prior to 112.0.5615.121
Product category:	Web browser
Severity:	CVSS: 8.8 | EPSS: 0.98%
Type:	Type confusion, heap corruption
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-2033 is a vulnerability that involves type confusion in V8 in Google Chrome versions prior to 112.0.5615.121. It allows a remote attacker to potentially exploit heap corruption via a crafted HTML page. The severity of this vulnerability is rated high by Chromium, with a CVSS v3.x base score of 8.8, indicating a high level of severity. This vulnerability is listed in CISA's Known Exploited Vulnerabilities Catalog, and the recommended action is to apply updates as per vendor instructions.

CVE-2023-2868

Affected products:	Barracuda Email Security Gateway
Product category:	Email security
Severity:	CVSS: 9.8 | EPSS: 1.64%
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

CVE-2023-2868 is a remote command injection zero-day vulnerability that affects the Barracuda Email Security Gateway appliance. This vulnerability is caused by a failure to comprehensively sanitize the processing of .tar files. An attacker can exploit this vulnerability by creating a malicious .tar file and sending it to a user of the appliance. When the user opens the .tar file, the attacker's malicious code will be executed on the appliance. Barracuda has released a patch for this vulnerability.

CVE-2023-34362

Affected products:	All MOVEit Transfer versions
Product category:	File transfer software
Severity:	CVSS: 9.8 | EPSS: 81%
Type:	SQL injection
Impact:	Unauthorized data access
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-34362 is a critical SQL injection vulnerability in Progress MOVEit Transfer software. This vulnerability could allow an attacker to execute arbitrary SQL commands on the MOVEit Transfer server, which could allow them to steal sensitive data, such as user passwords and credit card numbers, or to modify or delete data. Progress has released a patch for this vulnerability, and organizations that use MOVEit Transfer are advised to apply the patch as soon as possible.

CVE-2023-28252

Affected products:	All supported versions of Windows servers and clients
Product category:	Operating system
Severity:	CVSS: 7.8 | EPSS: 23.73%
Type:	Privilege escalation, out-of-bounds write (increment) vulnerability
Impact:	Confidentiality, integrity, availability
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

Microsoft has responded to this actively exploited zero-day vulnerability by taking decisive measures and releasing a patch to resolve it. This vulnerability enables unauthorized privilege escalation. In the event that a malicious actor obtains system access and possesses the ability to execute code, they can leverage this vulnerability to acquire SYSTEM privileges. These privileges represent the utmost level of user authority within the Windows operating system.

CVE-2023-34364

Affected products:	Progress DataDirect Connect for ODBC prior to version 08.02.2770
Product category:	Data integration tool
Severity:	CVSS: 9.8 | EPSS: 0.13%
Type:	Buffer overflow, code execution
Impact:	Confidentiality, integrity, availability
PoC:	No
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

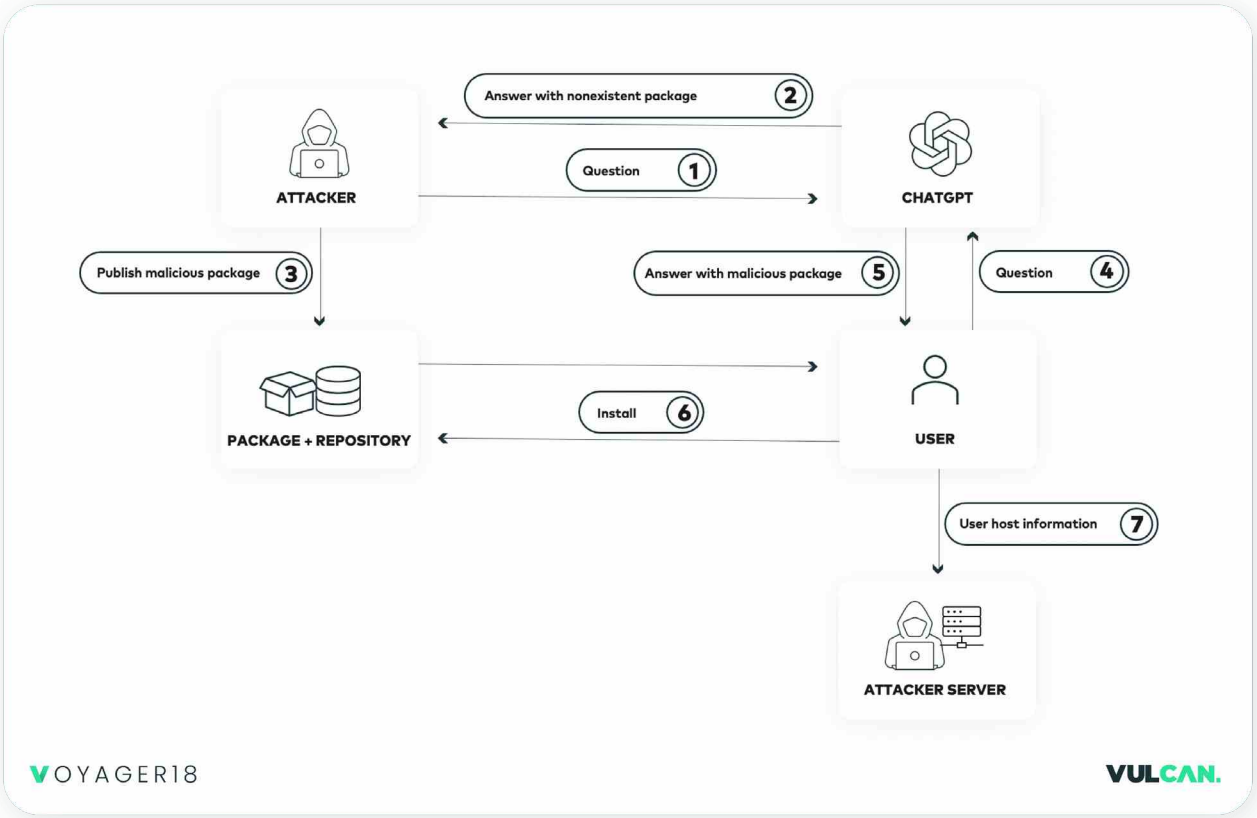
This vulnerability is due to the possibility of buffer overflow when a certain connection string option is given an overly large value. Such an overflow could potentially allow a malicious entity to inject and run their own code on the target system. Moreover, in those versions prior to 08.02.2770 (B1532, U1315), a security flaw exists when using Oracle Advanced Security (OAS) encryption. If an error arises during the initialization of an encryption object, a fallback mechanism is triggered. However, this mechanism uses an insecure random number generator to form the private key. This could enable an informed attacker to foresee the generated output.

AI package hallucination

Affected products:	Chat GPT, GPT3.5
Product category:	Generative AI
Severity:	N/A
Type:	LLM risk
Impact:	Can allow an attacker to spread malicious packages via ChatGPT
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	N/A
Remediation action:	Read more
MITRE advisory:	No

The rapid adoption of generative AI tools has presented a unique challenge for cyber security professionals, as shown by our team with a proof-of-concept of what we are terming "AI package hallucination".

ChatGPT - along with other generative AI tools - has a propensity for producing hallucinated facts and figures. As we have been able to demonstrate, it can also suggest non-existent packages when prompted for coding solutions. These imagined packages are a golden opportunity for attackers, who can produce them as disguised malware and upload them to coding repositories. When an unsuspecting user asks ChatGPT for development recommendations, these malicious packages may appear in the suggestions. It is easy to imagine what happens next, with these AI hallucinations potentially turning into real cyber risk.



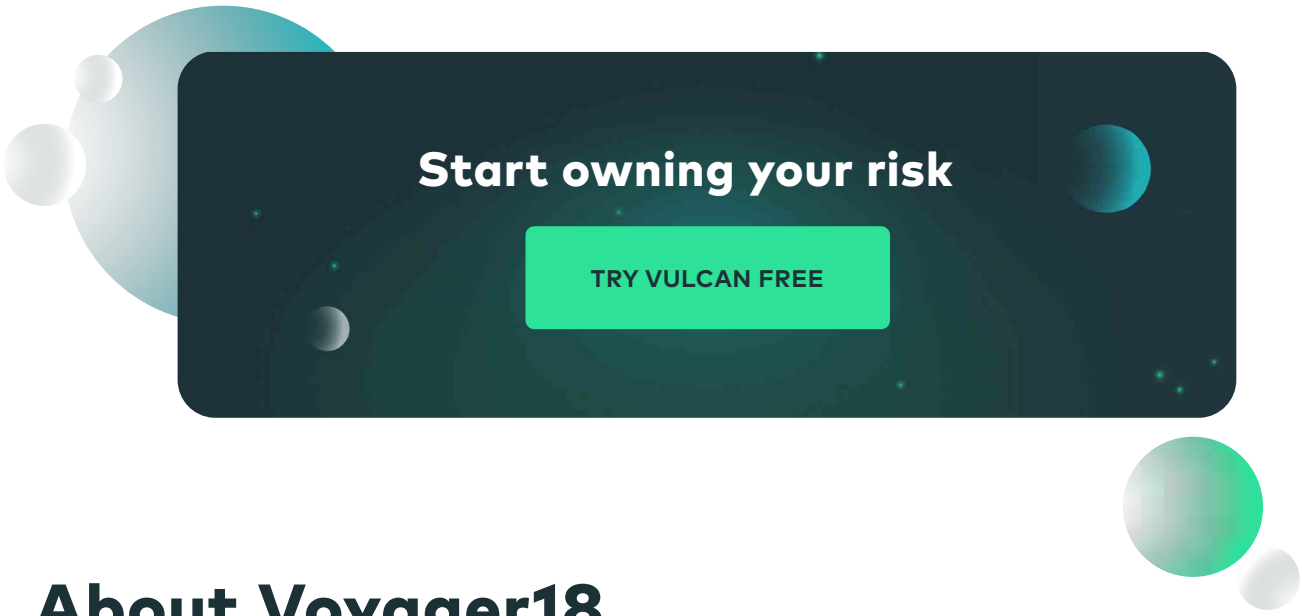
Validating suggestions from ChatGPT and other AI solutions is critical, particularly as dependence on them to ease workloads becomes more widespread.

Summary

In order to navigate the ever-changing landscape of cyber threats, organizations must prioritize staying abreast of emerging trends in cybersecurity, implementing a proactive vulnerability management strategy, and investing in ongoing training and education for their IT teams. By embracing these measures, organizations can successfully minimize the potential impact of vulnerabilities and uphold a robust security stance against persistent cyber challenges.

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 and as a 2020 RSA Conference Innovation Sandbox finalist. Prominent security teams, such as those at Mandiant, Deloitte, and Snowflake, trust Vulcan Cyber to help them own their risk.



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. The team is also responsible for bringing innovation to the Vulcan Cyber platform so that our customers get improved and customized cyber risk management capabilities. This includes research of more specific and accurate risk calculations, and the launch of VulnRX — a dynamic library of vulnerabilities and their remediation actions. Recently, the team mapped out the MITRE ATT&CK framework to relevant CVEs, providing granular insights into the most critical vulnerabilities. The full research is available here.

Stay up to date with the latest research here >>