Rezilion

REZILION 2023 FIRST-HALF CRITICAL VULNERABILITIES REPORT: Key Software Applications Under Fire

Introduction

SOFTWARE CAN PRESENT A MAJOR RISK FOR CYBERSECURITY EXECUTIVES TODAY. Vulnerabilities continue to plague enterprises and small organizations alike, and researchers are regularly discovering new flaws.

Cybercriminals and other bad actors can exploit many of these software vulnerabilities to launch attacks against organizations, their customers, and even entire supply chains. In recent years, several incidents involving weaknesses in software code were used as launching points for attacks such as ransomware.

Security risks related to software come from a variety of sources, including the software manufacturers themselves. For example, vulnerabilities can be introduced during the development process, in open source software, in software supply chains, and through other means.

Regardless of where vulnerabilities come from, security leaders and teams need to be aware of the latest vulnerabilities so that they can take the necessary steps to ensure security. Some reported vulnerabilities can have serious consequences for organizations; others can be much less impactful.

This report, based on research by Rezilion, describes some of the notable and critical vulnerabilities from the first half of 2023. It provides relevant remediation and mitigation steps as needed.

JsonWebToken: CVE-2022-23529

A VULNERABILITY THAT NEVER REALLY WAS, CVE-2022-23529 was published in December 2022 with a Common Vulnerability Scoring System (CVSS) score of 9.8 and was described as a critical vulnerability in the popular JsonWebToken open source project.

In January 2023, Palo Alto researchers released their findings detailing the necessary prerequisites for the vulnerability to be successfully exploited in affected products.

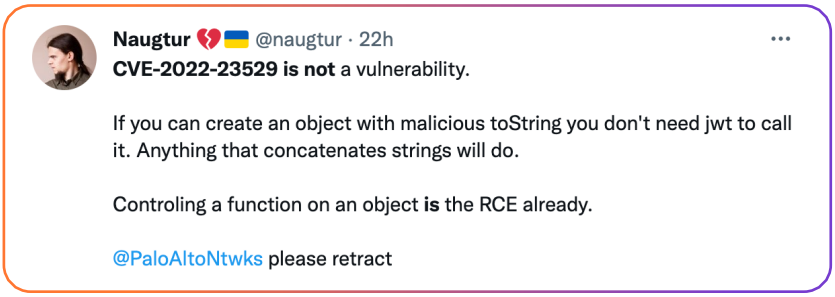
Since then, doubts have emerged regarding both the exploitation prerequisites and the vulnerability itself. Rezilion researchers investigated the chances of exploiting the vulnerability. They found that although the vulnerability received a CVSS score of 9.8, the chances for the preconditions needed to exploit the vulnerability in real-world applications were slim.

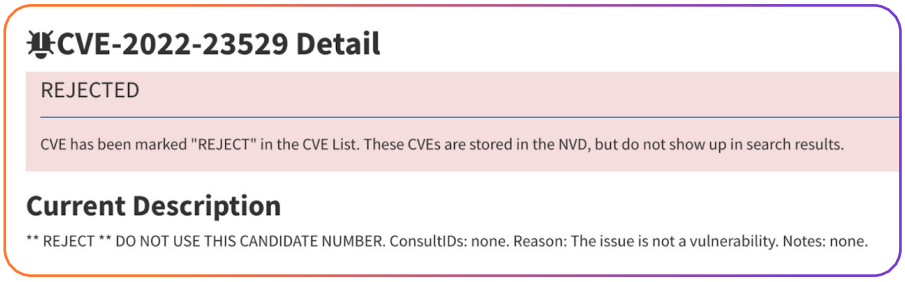
To exploit the vulnerability, they said, two key conditions need to be met:

- ✓ A server does not store secret keys securely.
- ✓ The attacker needs to have access to and control of the secret keys.

Given these requirements, an application would be insecure in a way that allows an attacker to exploit it regardless of the vulnerability.

In January 2023, the vulnerability was rejected by the National Vulnerability Database operated by the National Institute of Standards and Technology (NIST).





Palo Alto researchers posted that they decided to retract CVE-2022-2352 after hearing the community's feedback about the needed prerequisites to exploit the vulnerability.

It's impressive and encouraging to see the research community's dedication to scrutinizing vulnerabilities and not accepting them at face value. The lesson learned is that doubts and critical analysis play crucial roles in ensuring accurate assessments and mitigations. By questioning and examining vulnerabilities, researchers can contribute to the overall security ecosystem and help maintain a high level of reliability and trust in software systems.

ChatGPT: CVE-2023-28858

CVE-2023-28858, PUBLISHED IN MARCH 2023 WITH A CVSS SCORE OF 3.7, affected the OpenAI ChatGPT service, which needed to shut down to fix the issue. The vulnerability was discovered in the Redis open source library and specifically affected OpenAI's ChatGPT payment accounts, resulting in a leak of user data.

While this vulnerability has a low severity score, it is significant in the context of increased reliance on these types of artificial intelligence (AI) services. As AI technology continues to advance and more enterprises rely on it, it's crucial to acknowledge and address security concerns from the beginning. This sets the stage for future discussions and proactive measures to ensure the safety and integrity of AI systems.

Redis is an in-memory data structure store commonly used as a database, cache, and message broker, and the vulnerability affects all versions of Redis prior to 4.5.3. When a client sends a command to Redis, it waits for the response before sending another command. But Redis supports pipelining, which allows clients to send multiple commands at once without waiting for a response. This can improve performance by reducing the number of round trips between the client and Redis.

Sometimes when a client cancels an async Redis command, it leaves the connection open. This can happen in the case of a pipeline operation where multiple commands are sent at once. If one command is canceled, it can leave the connection open, meaning the server is still waiting for a response.

If the server sends a response to this connection, it can be received by the client of an unrelated request. This means the response data is sent to the wrong client, which can result in unexpected behavior and data leaks. There's a window between when the client sends the command and when the client receives the response. In this window, if the client cancels the async command, the connection remains open and another user will receive the response instead.

Redis has fixed the issue, ensuring that data is properly drained from asynchronous connections when a session is disconnected and that responses are only sent to the intended clients.

REMEDIATION

Organizations using the Redis platform need to update to one of the following versions: 4.3.6, 4.4.3, or 4.5.3.

As for ChatGPT, while it is not directly related to Redis, OpenAI has taken measures to ensure that user data is kept private and secure. This includes making changes to the way data is sent to clients to make sure that it's only relevant to them and preventing any potential data leaks.

Apache Superset: CVE-2023-27524

IN APRIL 2023, HORIZON3.AI ANNOUNCED THE DISCOVERY OF CVE-2023-27524, a critical vulnerability in Apache Superset with a CVSS score of 9.8. The vulnerability was caused by the use of the default SECRET_KEY configuration generated by the application rather than generating a new unique key or taking action when this type of configuration is applied.

Using the default SECRET_KEY is not secure; it is publicly available, and attackers can easily discover it. Once attackers obtain the key, they can generate a cookie and sign it using the key, allowing them to gain unauthorized access to the application.

In response to the vulnerability, the development team at Horizon3.ai took significant measures to address the issue. They implemented a fix that involved preventing a server from starting if it's configured to deploy with the default SECRET_KEY, starting with version 2.1 of Apache Superset.

This change requires users to generate and use their own unique SECRET_KEY, ideally one that is strong enough to resist attacks such as the one that led to the discovery of the vulnerability. It is important to note that this patch does not cover all use cases, however, as users can still install Superset with a default SECRET_KEY if it is done through a docker-compose file or a helm template.

Organizations using Apache Superset server or other applications that use Flask session cookies should take the following steps:

- Execute this script to see if the Apache Superset server is running with an insecure default configuration.
- If using a vulnerable version of Apache Superset, Apache Airflow, or Redash, upgrade to the fixed versions and update all keys.
- In Apache Superset, follow these instructions to rotate the SECRET_KEY, making sure to use strong keys that cannot be easily cracked.
- If using Apache Superset via docker-compose, ensure that the fix isn't already applied and generate a new SECRET_KEY.
- To avoid potential attacks, do not expose servers to the internet and monitor for any suspicious activity.
- If using any other application that employs Flask session cookies and allows the default SECRET_KEY, contact the application's developers and suggest implementing the same approach of refusing to start the server if it is configured to deploy with the default SECRET_KEY.
- Always use a strong, unique key to protect the application.

REMEDIATION

Organizations using any of the versions affected by the vulnerabilities should upgrade to the latest version immediately. Here are the affected versions for each CVE:

- **CVE-2023-27524: Apache Superset is vulnerable in versions up to and including 2.0.1.**
- **CVE-2021-41192: Redash is vulnerable in versions up to and including 10.0.0.**
- **CVE-2020-17526: Apache Airflow is vulnerable in versions up to but including 1.10.13.**

PaperCut: CVE-2023-27350

CVE-2023-27350, REPORTED BY THE ZERO DAY INITIATIVE AND PUBLISHED IN MARCH 2023, is an actively exploited remote code execution (RCE) vulnerability in print management applications PaperCut NG and PaperCut MF. It has a CVSS score of 9.8.

PaperCut is used by organizations of all sizes and provides features for print job tracking, quotas, and rules-based printing. The vulnerability stems from an access control issue within the SetupCompleted java class in the pcng-server-web jar file. It's a session variable overloading vulnerability that arises when an application assigns the same session variable — such as "userid" — with a user's username upon login and subsequently uses this variable in database queries to retrieve user-specific data.

The application does not perform additional checks to ensure that the user is authenticated and authorized to access the requested resources.

In CVE-2023-27350, the SetupCompleted class has a function called formSubmit that calls the getSetupData function without confirming that the user is logged in. It then calls the performLogin function with admin permissions. Since the user is not confirmed to be logged in, an attacker can easily bypass the authentication and access the page with admin permissions.

After successfully bypassing the authentication, an attacker can create scripts in PaperCut and execute code with system privileges on the affected PaperCut server.

With the fix, before calling the performLogin function with admin permissions, formSubmit now calls the getSetupData function with the isConfirmed function to validate that a user was authenticated. If the code finds that the user is not authenticated, it sends the user back to the web homepage.

REMEDIATION

The first version in each range is affected by the vulnerability, and the second version in each range is patched and not affected:

- ✓ **PaperCut MF/PaperCut NG - 8.0.0 through 20.1.7**
- ✓ **PaperCut MF/PaperCut NG - 21.0.0 through 21.2.11**
- ✓ **PaperCut MF/PaperCut NG - 22.0.0 through 22.0.9**

Organizations that have affected versions of PaperCut MF/NG need to patch immediately to one of the following versions: 20.1.7, 21.2.11, 22.0.9. If they're unable to patch, they should ensure that vulnerable servers are not exposed to the internet.

Since this vulnerability is actively exploited in the wild, organizations using these print management applications should assume compromise and look for any abnormal activity that could be associated with exploitation attempts. More guidelines and updates can be found in the Cybersecurity & Infrastructure Security Agency (CISA) and FBI advisory.

Fortinet FortiOS: CVE-2022-41328

CVE-2022-41328 IS A ZERO-DAY VULNERABILITY IN THE FORTINET FORTIOS that is known to be exploited in the wild by threat actors. It has a CVSS score of 7.1.

As of May 2023, the CISA had reported 10 Fortinet FortiOS known exploited vulnerabilities. Threat actors that exploited the vulnerabilities installed malware that is designed to establish contact with a remote server to download files, exfiltrate data from the compromised host, and grant remote shell access.

Government entities and large organizations have been targeted by the vulnerability, and results have included data loss and operating system and file corruption.

This is a path traversal vulnerability caused by an improper limitation of a pathname to a restricted directory. A privileged attacker successfully exploiting the vulnerability can read and write files on the underlying Linux system via crafted command-line interface commands.

REMEDIATION
Fortinet provides further analysis of the attack and detection indicators, and suggested remediation is to upgrade FortiOS to one of these versions: 6.2.14, 6.4.12, 7.0.10, 7.2.4, or above.

Adobe ColdFusion: CVE-2023-26360

CVE-2023-26360 IS A CRITICAL, RCE ZERO-DAY VULNERABILITY in Adobe ColdFusion with a CVSS score of 9.8. It's known to be exploited in the wild in limited attacks.

The vulnerability is a deserialization of untrusted data vulnerability in Adobe ColdFusion 2021 Update 5 and earlier versions as well as ColdFusion 2018 Update 15 and earlier versions. An attacker successfully exploiting the vulnerability can remotely execute code on affected systems.

REMEDIATION
There is a published metasploit module that exploits the vulnerability to gain RCE. Recommended remediation is to update ColdFusion to these versions: 2021 release Update 6 and 2018 release Update 16.

Conclusion

SECURITY LEADERS AND TEAMS CANNOT AFFORD TO FALL BEHIND CYBERCRIMINALS AND OTHER BAD ACTORS who are determined to leverage software vulnerabilities to launch attacks. The sooner they learn about potentially damaging bugs, the earlier they can formulate a plan of action to defend their organizations.

Some of the software that was affected in the first half of 2023 play important roles in organizations, providing capabilities such as data analytics and visualization, AI, web development, and cybersecurity.

Part of due diligence is keeping up with the latest exploitable bugs so that security teams can take proper remediation actions before it's too late. By reviewing the vulnerabilities outlined in this report, cybersecurity leaders and teams can do what is necessary to protect their organizations.

About Rezilion

Rezilion's software supply chain security platform automatically assures that the software you use and deliver is free of risk. Rezilion detects third-party software components on any layer of the software stack and understands the actual risk they carry, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable risk across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's platform at www.rezilion.com and get a 30-day free trial.