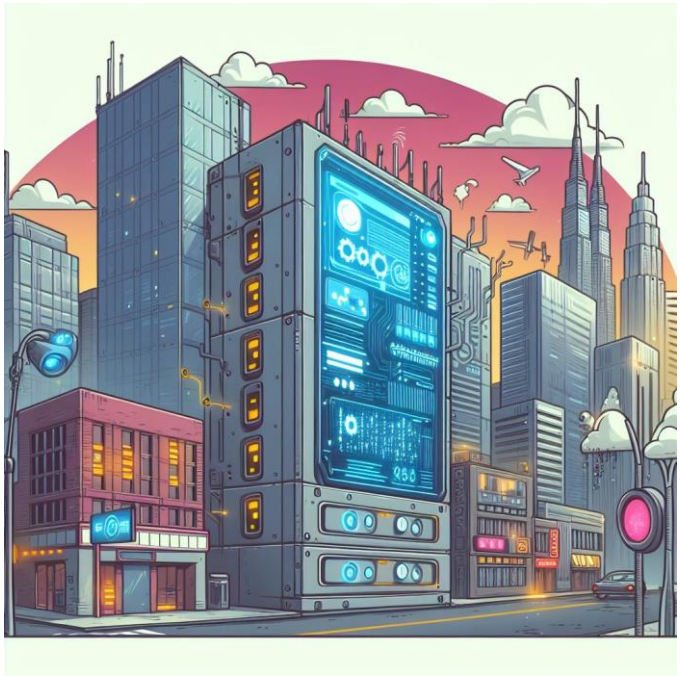

Abstract – This document presents a analysis of CVE-2023-22518, an improper authorization vulnerability in Atlassian Confluence Data Center and Server. The analysis will cover various aspects of the vulnerability, including its discovery, impact, exploitation methods, and mitigation strategies.

Security professionals will find the analysis particularly useful as it offers actionable intelligence, including indicators of compromise and detailed mitigation steps. By understanding the root causes, exploitation methods, and effective countermeasures, security experts can better protect their organizations from similar threats in the future.

I. Introduction

CVE-2023-22518 is an improper authorization vulnerability that affects all versions of Confluence Data Center and Server. This vulnerability allows an unauthenticated attacker to reset Confluence and potentially take control of an affected system. It was first disclosed by Atlassian on Oct 31, 2023.

The vulnerability was initially rated with a critical severity score of 9.1 in the Common Vulnerability Scoring System (CVSS), but it was later escalated to 10, the highest critical rating, due to the change in the scope of the attack and the observation of active exploits and reports of threat actors using ransomware.

The vulnerability has been observed to be exploited by a threat group known as 'Storm-0062'. As of November 5, 2023, there have been confirmed instances of active exploitation of CVE-2023-22518.

Atlassian has released fixed versions of Confluence to address CVE-2023-22518. The fixed versions are 7.19.16, 8.3.4, 8.4.4, 8.5.3, and 8.6.1. Additionally, restricting external access to Confluence servers until the update can be applied is recommended. Atlassian Cloud users are not affected by this vulnerability.

II. Attacks Details

The vulnerability was discovered through a patch diff between the patched and unpatched versions of the software. The researchers identified the addition of two new annotations, namely, @WebSudoRequired and @SystemAdminOnly, in various Action classes.

The vulnerability lies in the "setup restore" endpoints on Confluence instances, which were accessible to unauthenticated users. The setup-restore endpoints in Atlassian Confluence Data Center and Server are part of the system's restore functionality. These endpoints are intended to be used by administrators to restore a Confluence instance from a backup

The endpoints that only the administrator user should be able to access include /json/setup-restore.action, /json/setup-restore-local.action, and /json/setup-restore-progress.action. Using these, an adversary can upload a specially crafted .zip archive file using an HTTP Post request. The zip file can contain a web shell, allowing to execute arbitrary commands.

A. *Attack flow*

The attack flow of CVE-2023-22518 involves several steps that allow an unauthenticated attacker to exploit improper authorization vulnerabilities within Confluence Data Center and Server:

- **Exploitation of "Setup Restore" Endpoints**: The attacker targets the "setup restore" endpoints in Confluence, which are intended for administrators to restore a Confluence instance from a backup. These endpoints include /json/setup-restore.action, /json/setup-restore-local.action, and /json/setup-restore-progress.action. Due to the vulnerability, these endpoints are accessible to unauthenticated users
- **Uploading a Malicious .zip File**: The attacker crafts a specially designed .zip file that, when uploaded to the vulnerable Confluence server through the compromised endpoints, can either destroy the Confluence instance, leading to data loss, or contain a web shell for achieving remote code execution (RCE) on the server
- **Gaining Unauthorized Access**: If the attack involves uploading a web shell, the attacker can execute arbitrary commands on the server. This level of access allows the attacker to perform all administrative actions that are available to Confluence instance administrators, effectively taking control of the system
- **Deployment of Ransomware**: In some cases, the attackers have used this vulnerability to deploy ransomware, such as Cerber ransomware. Upon execution, the ransomware encrypts files on local disks and network shares, appending a specific file extension (e.g., .LOCK3D) to encrypted files, and demands a ransom to decrypt the data
- **Consequences**: Successful exploitation of CVE-2023-22518 can lead to unauthorized system control, data loss, operational disruption, and financial costs due to ransomware deployment. The attackers can disrupt operations, access sensitive information, and manipulate or delete critical data

B. PoC

The exploit.py file from the GitHub repository https://github.com/ForceFledgling/CVE-2023-22518 performs the following actions:

- **Target Identification**: The script would prompt the user to input the URL of the vulnerable Confluence instance.
- **Exploit Execution**: The script would then use the provided URL to send crafted requests to the "setup restore" endpoints, such as /json/setup-restore.action, which are normally restricted to administrators but were exposed to unauthenticated users due to the vulnerability.
- **Malicious Payload Upload**: The exploit would involve uploading a malicious .zip file that could contain a web shell or other malicious code to the server via the compromised endpoints.
- **Remote Code Execution (RCE)**: If the uploaded .zip file contains a web shell, the attacker could execute arbitrary commands on the server, leading to unauthorized system control.
- **Outcome**: The successful execution of the script result in the attacker gaining administrative access to the Confluence instance, which could be used to perform further malicious activities, such as data exfiltration, data destruction, or ransomware deployment.

Incoming data for the script would include the URL of the target Confluence instance and the path to the malicious .zip file. Outgoing data would consist of HTTP requests to the vulnerable endpoints and potentially the uploaded malicious payload.

The xmlexport-20231109-060519-1.zip is a malicious .zip file used in conjunction with the exploit script for CVE-2023-22518. This file is intended to be uploaded to a vulnerable Confluence Data Center and Server instance to exploit the improper authorization vulnerability. When uploaded to a vulnerable Confluence instance, it could lead to unauthorized file uploads, potentially enabling remote code execution or other security vulnerabilities.

Additionally, in the context of exploiting CVE-2023-22518, a .jar file like atlplug.jar could serve as Confluence Backdoor Shell App to perform specific actions on a vulnerable Confluence server.

III. Affected Industries

Atlassian Confluence is used across a wide range of industries due to its versatility as a team collaboration software. It is particularly prevalent in the following sectors:

- **Information Technology and Services**: Confluence is heavily utilized in the IT sector for knowledge management, documentation, and collaboration on software development projects
- **Computer Software**: Many software development companies use Confluence to manage their product documentation, track project progress, and facilitate communication among team members
- **Financial Services**: The financial industry employs Confluence to organize sensitive information, maintain compliance documentation, and support internal collaboration
- **Education**: Educational institutions may use Confluence as a knowledge base for IT support, as well as for managing and sharing edu materials and research
- **Government**: Government agencies can use Confluence to manage projects, documentation, and to create a centralized repository for institutional knowledge
- **Healthcare**: Healthcare organizations might use Confluence for managing patient information systems, research documentation, and as a knowledge base for medical staff

A. Impact

These industries relies heavily on Confluence for project management, documentation, and collaboration. The exploitation of CVE-2023-22518 can lead to:

- **Unauthorized System Control**: Attackers can gain administrative access, allowing them to perform any actions within the Confluence instance, which could disrupt operations and compromise sensitive data
- **Ransomware Deployment**: There have been instances where the vulnerability was used to deploy Cerber ransomware, leading to data encryption and ransom demands, which can halt IT operations and lead to financial losses
- **Operational Disruption**: The reset of a Confluence instance can disrupt ongoing projects and collaboration efforts, leading to delays and potential loss of data

B. Consequences

Consequences for these industries:

- **Data Loss**: Unauthorized access and potential ransomware deployment can result in irreversible data loss, which is particularly damaging in an industry that relies on data integrity
- **Financial Costs**: The costs associated with ransomware demands, system recovery, and potential regulatory fines can be substantial
- **Reputation Damage**: Security breaches can damage the reputation of IT service providers, leading to loss of trust and potential loss of business
- **Resource Allocation**: IT departments may need to redirect resources to address the vulnerability and its fallout, which can detract from other critical IT initiatives