

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Active Exploitation of Two Critical Flaws in Microsoft SharePoint

Date of Publication

January 15, 2024

Admiralty Code

A1

TA Number

TA2024015







Summary

First Seen: September 2023

Affected Platform: Microsoft SharePoint Server

Impact: Active attacks targeting a critical Microsoft SharePoint Server vulnerability (CVE-2023-29357) pose a severe risk, enabling privilege escalation for potential full administrator access. This flaw, coupled with CVE-2023-24955, allows arbitrary code execution. Immediate patching is crucial, as fixes have been available since June 2023's Patch Tuesday.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-29357	Microsoft SharePoint Server Privilege Escalation Vulnerability	Microsoft SharePoint Server			
CVE-2023-24955	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server			

Vulnerability Details

#1

A critical vulnerability (CVE-2023-29357) in Microsoft SharePoint, allows remote attackers to gain admin privileges on unpatched servers by using spoofed JWT (JSON Web Token) authentication tokens to circumvent authentication. Once exploited, attackers can execute network attacks without requiring user action, potentially leading to the acquisition of administrator privileges.

#2

Furthermore, when combined with another critical vulnerability (CVE-2023-24955) in SharePoint Server, attackers can execute arbitrary code on compromised servers through command injection. This exploit chain was demonstrated successfully in the March 2023 Pwn2Own contest by a researcher from STAR Labs, earning a \$100,000 reward. Subsequently, a proof-of-concept exploit for CVE-2023-29357 was released on GitHub, allowing attackers to identify admin users with elevated privileges.

#3

Although the released exploit lacks remote code execution capabilities, threat actors can combine it with CVE-2023-24955 for full exploitation. Several other proof-of-concept exploits for this chain have emerged online, potentially lowering the skill threshold for attackers. CISA has included the vulnerability in its Known Exploited Vulnerabilities Catalog and mandated U.S. federal agencies to patch it by January 31, indicating the severity and urgency of the situation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-29357	Microsoft SharePoint Server: 2019	cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*	CWE-287
CVE-2023-24955	Microsoft SharePoint Server: 2016, 2019, Subscription Edition All versions	cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:subscription_edition:*:*:*:*:*:*	CWE-94

Recommendations



Apply Patch and Update: Apply the latest security patches and updates provided by Microsoft for SharePoint Server promptly. Ensure that both the SharePoint Server and any related components are running the latest versions with all available security fixes.



JWT Token Validation: Enhance JWT token validation mechanisms to detect and prevent the use of spoofed tokens. Implement additional authentication controls to ensure the integrity of JWT tokens.



Deploy Anomaly Detection and Monitoring: Implement network monitoring tools with anomaly detection capabilities to identify unusual or suspicious patterns of network activity. This can include unexpected increases in data traffic, unusual access patterns, or deviations from normal behavior.



Network Segmentation: Employ network segmentation to isolate email security appliances from critical internal networks. This can help contain the impact of a potential breach and prevent lateral movement within the network.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>TA0004</u> Privilege Escalation
<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities	<u>T1659</u> Content Injection	<u>T1588</u> Obtain Capabilities
<u>T1134</u> Access Token Manipulation	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1190</u> Exploit Public-Facing Application	<u>T1059</u> Command and Scripting Interpreter

Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955>

References

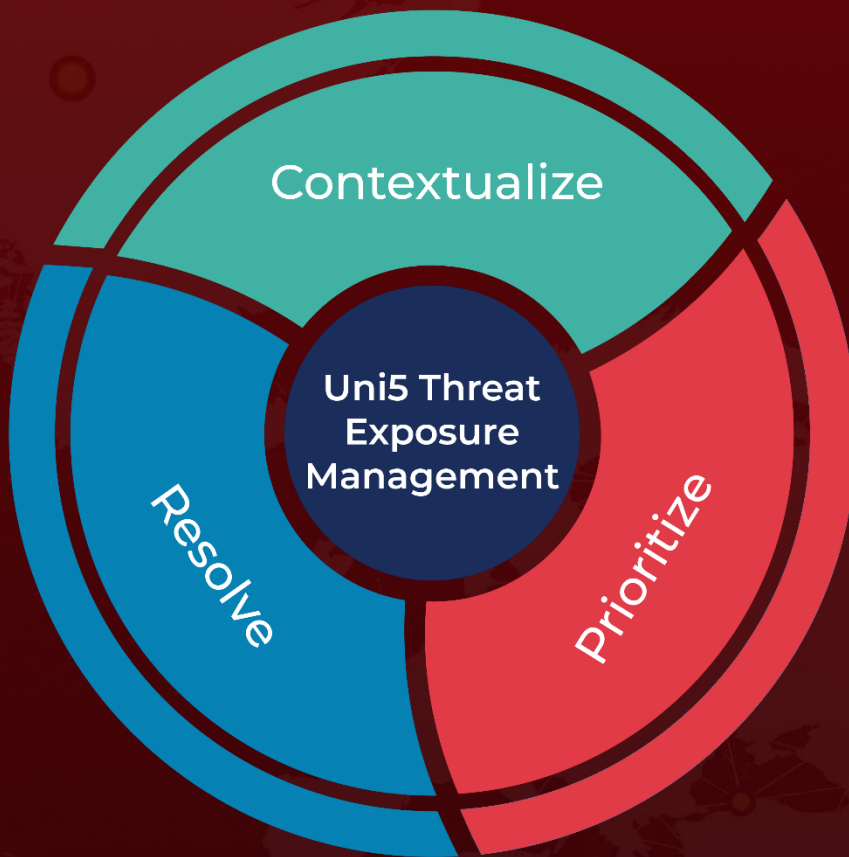
<https://www.cisa.gov/news-events/alerts/2024/01/10/cisa-adds-one-known-exploited-vulnerability-catalog>

<https://thehackernews.com/2024/01/act-now-cisa-flags-active-exploitation.html>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

January 15, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro[®]



More at www.hivepro.com