



| Flash |

Critical Microsoft SharePoint Vulnerability Actively Exploited

F-2024-01-15a

Classification: TLP:CLEAR

Criticality: Medium

**Intelligence Requirements: Vulnerability Exploitation, Deep Dark
Web & Criminal Underground**

January 15, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EST) on January 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Critical Microsoft SharePoint Vulnerability Actively Exploited

› Key Findings

- Critical severity Microsoft SharePoint privilege escalation vulnerability CVE-2023-29357 has been added to the U.S. Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog, indicating it is being actively exploited in cyber attacks.
- The vulnerability can be exploited alongside Remote Code Execution (RCE) vulnerability CVE-2023-24955, forming an attack chain able to further compromise the confidentiality, integrity, and availability of a target system.
- ZeroFox urges users to ensure networks are patched with the latest Microsoft software updates.

| Details

On January 10, 2024, CISA added CVE-2023-29357—a critical severity privilege escalation flaw in Microsoft SharePoint—to its Known Exploited Vulnerabilities Catalog, indicating its active exploitation in the wild.¹ CVE-2023-29357 enables threat actors targeting unpatched servers to obtain administrator privileges, facilitating follow-on malicious activity and lateral movement. The vulnerability has been assigned a critical CVSS score of 9.8 out of 10.

¹ [hXXps://www.cisa\[.\]gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

- The flaw enables unauthenticated threat actors to impersonate any SharePoint user by spoofing valid JSON Web Tokens (JWT), circumventing signature validation checks for authentication.
- There is a roughly even chance that the vulnerability has been previously leveraged against unpatched networks without being brought to the attention of Microsoft or security researchers.
- Successful exploitation requires no initial privileges or any action from the victim.
- A security update addressing CVE-2023-29357 was released by Microsoft as early as June 13, 2023.²³

Since then, however, proof of concepts (PoCs) published detail an exploitation chain which also leverages Microsoft vulnerability CVE-2023-24955.⁴⁵

- CVE-2023-24955 is a Microsoft SharePoint Remote Code Execution (RCE) security flaw with a CVSS score of 7.2.
- Used in conjunction with privilege escalation obtained through the leveraging of CVE-2023-29357, attacks are able to further compromise the confidentiality, integrity, and availability of a target system.

A threat actor leveraging this attack chain to gain unauthorized access and administrator privileges could deploy malicious payloads to the network, such as ransomware or data stealing malware. Threat actors could also conduct lateral movement to gain access to more sensitive or critical parts of the network. Threat actors will likely continue leveraging this attack chain against unpatched networks in the short term.

- Threat actors likely become increasingly aware of vulnerabilities in the wild following the publishing of PoCs, which although written “ethically”, may provide insight into specific attack chains.

² [hXXps://nvd.nist\[.\]gov/vuln/detail/CVE-2023-29357](https://nvd.nist.gov/vuln/detail/CVE-2023-29357)

³ [hXXps://msrc.microsoft\[.\]com/update-guide/en-US/vulnerability/CVE-2023-29357](https://msrc.microsoft[.]com/update-guide/en-US/vulnerability/CVE-2023-29357)

⁴ [hXXps://starlabs\[.\]sg/blog/2023/09-sharepoint-pre-auth-rce-chain/](https://starlabs[.]sg/blog/2023/09-sharepoint-pre-auth-rce-chain/)

⁵ [hXXps://github\[.\]com/Chocapikk/CVE-2023-29357](https://github[.]com/Chocapikk/CVE-2023-29357)

- As acknowledged by Microsoft's categorization of both CVE-2023-29357 and CVE-2023-24955's as "low" complexity, successful execution of the attack chain does not require sophisticated capabilities, resulting in low barriers to entry.⁶⁷ This very likely increases their appeal to threat actors of all capabilities and motivations.
- The likelihood of targeting is exacerbated by Microsoft SharePoint's widespread dispersion amongst organizations and their supply chains, and a very likely high number of unpatched networks.

| Recommendations

- Ensure networks are patched with the latest Microsoft software patches available from the MSRC Security Updates page, available at:
 - [hXXps://msrc.microsoft\[.\]com/update-guide/vulnerability/CVE-2023-24955](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955)
 - [hXXps://msrc.microsoft\[.\]com/update-guide/vulnerability/CVE-2023-29357](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357)
- Ensure a thorough understanding of organizational technology stacks, including those of operating partners.
- Consistently monitor for security patch releases impacting these products and deploy a holistic patch management system to ensure all business IT assets are updated with the latest software as quickly as possible.
- Conduct a thorough assessment of servers and review any relevant activity logs for suspicious behavior.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.
- Protect endpoint devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards.
- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures and key authorities.

⁶ [hXXps://msrc.microsoft\[.\]com/update-guide/vulnerability/CVE-2023-24955](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955)

⁷ [hXXps://msrc.microsoft\[.\]com/update-guide/en-US/vulnerability/CVE-2023-29357](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29357)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%