SWEY
CYBEREYE

REMOTE CODE EXECUTION IN MICROSOFT SHAREPOINT

IMAGE SOURCE: AMTRUSTFINANCIAL.COM

Hype Value	General Risk	Risk to EQT
Low	High	High

Title: Remote Code Execution in Microsoft SharePoint

Date: October 11, 2022

Threat description

A Remote Code Execution vulnerability was discovered in Microsoft's SharePoint application which when exploited could compromise the integrity and confidentiality of shared data on the said application. This weakness will allow attacker to remotely execute malicious codes on the SharePoint server. The attacker must first be authenticated to be able gain remote access to run the arbitrary code on the server. This vulnerability is as a result of improper validation of data supplied by users.

CVE Number	Description
CVE-2022-37961	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2022-38048	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2022-38009	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2022-38008	Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2022-35823	Microsoft SharePoint Server Remote Code Execution Vulnerability

Impact

This vulnerability could be exploited by the attacker to steal, delete, or encrypt sensitive information shared on the server, alter user permissions, or create backdoors.

Risk Assessment

Based on the following information, the risk to the client is high. This is because an exploitation of the said vulnerability could have catastrophic effects on the target organization. It will compromise the integrity and confidentiality of organization's data available on SharePoint. The attacker can encrypt the compromised shared data for a ransom, delete or leak files. The attacker can also modify the system configuration to alter user permissions.

Actions taken

1. Contacted the system administrator to run vulnerability scan on the company's SharePoint server to detect vulnerabilities.
2. Downloaded and installed security and cumulative updates for SharePoint servers.
3. Ran windows updates for all company's devices.
4. Updated the vulnerability scanning software.

Next Steps and Recommended Actions

1. Employ a monitoring system to detect abnormal behaviors that may lead to an attack.
2. Download and install windows updates in a timely manner

Sources

1. https://nvd.nist.gov/vuln/detail/CVE-2022-38048
2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38048
3. https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-sharepoint-server-subscription-edition-september-13-2022-kb5002271-9b21704b-ce7b-4da8-93e4-b0d6f9dbbd8d
4. https://blog.qualys.com/vulnerabilities-threat-research/2022/10/11/october-2022-patch-tuesday
5. https://thesecmaster.com/how-to-fix-cve-2022-35823-a-remote-code-execution-vulnerability-in-microsoft-sharepoint/

Metadata

Report date	28.10.22
Analyst	Stephen Mensah
History	V 1.0

SWEY
CYBEREYE

3519 52nd St
New York, NY 11053

+1 (719) 332 - 8997

info@sweycyber.com

www.sweycyber.com