Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

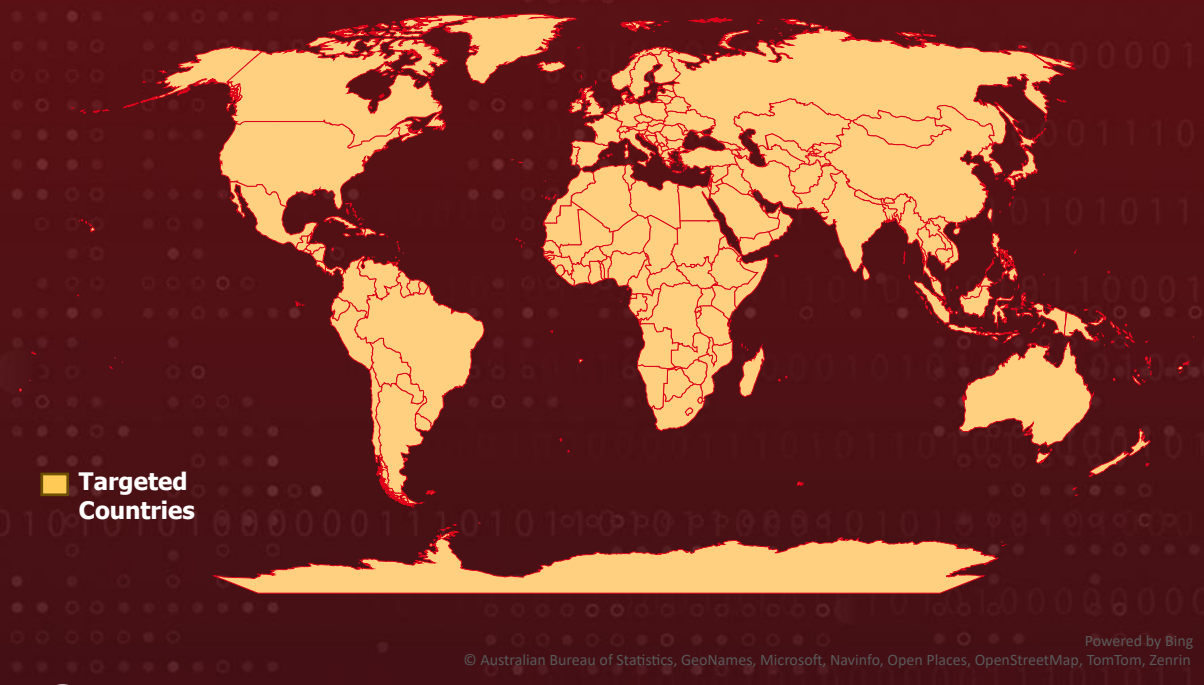
Threat Actors Weaponized SharePoint Flaw To Infiltrate Corporate Networks

Date of Publication	Admiralty Code	TA Number
November 07, 2024	A1	TA2024419

Summary

Attack Discovered: October 2024
CVE: CVE-2024-38094
Attack: Threat Actors have leveraged SharePoint Remote Code Execution Flaw, CVE-2024-38094, to infiltrate corporate networks and deployed a Fast Reverse Proxy and a custom webshell to maintain control over the compromised systems. Their innovative tactic involves installing unauthorized security software that conflicted with and disabled existing security solutions, showcasing their evolving methods to circumvent traditional defenses.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-38094	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✓	✓

Attack Details

#1 Threat actors leveraged a critical vulnerability in Microsoft SharePoint, identified as CVE-2024-38094, to gain unauthorized access to corporate networks. Attackers installed a webshell on SharePoint servers and also maintained persistence by deploying a Fast Reverse Proxy on domain controllers. They exploited access to a Microsoft Exchange service account to move laterally across the network, compromising the entire domain.

#2 CVE-2024-38094 is a high-severity remote code execution flaw affecting Microsoft SharePoint, this flaw enables authenticated users with Site Owner permissions to inject and execute arbitrary code within the SharePoint environment. CVE-2024-38094 can be exploited over the network but requires authentication as a highly privileged user. A proof-of-concept (PoC) exploit is publicly available, and Microsoft has addressed this vulnerability with a patch released in July 2024.

#3 The attack began with the exploitation of CVE-2024-38094, allowing the attackers to gain initial access to the network. They then deployed a web shell on the SharePoint server to ensure persistent access. They executed mimikatz for credential harvesting and tampered with system log to conceal their activities.

#4 Following this, the attackers moved to the domain controller, utilizing the Exchange service account, which also had Domain Administrator privileges. They installed a Fast Reverse Proxy (FRP) on domain controller, enabling external access to the compromised system. Persistence for the FRP was established through scheduled tasks on the domain controller, allowing the attackers to maintain their foothold and control over the network.

#5 They employed multiple tools with capability to map Active Directory environment, gather credentials, brute force Active Directory Kerberos tickets, mapping NTFS file system and even attempted to compromise backup solution.

#6 The attacker demonstrated operational excellence by swiftly switching techniques after Impacket blocked execution. They crashed the existing security solution by creating a conflict with a second antivirus system, effectively disabling it. This innovative approach highlights the continuous evolution of attacker tactics, allowing them to maintain persistence and control over the compromised environment while evading detection.

Recommendations

Patch Your System Immediately: Ensure that all SharePoint servers are updated to the latest build, as promptly applying security updates will help keep you one step ahead of attackers.

Threat Exposure Management: Perform an exposure assessment to identify exploitable flaws and prioritize internet-facing services based on publicly known exploits. This proactive approach will help catch vulnerabilities like CVE-2024-38094 early, thereby protecting us from a full-blown incident.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence or Actors activity. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Adhere to Idea of Least Privilege: Ensure that Service accounts are granted only the necessary permissions for their specific functions. Employ the delegated rights feature wherever feasible. This proactive approach can significantly enhance security by scoping and limiting any successful intrusion, thereby thwarting lateral movement and preventing the compromise of the entire infrastructure.

Monitor and Respond: Utilize a SIEM solution to monitor critical incident events, including antivirus software crashes, deletion of system logs, and blocked security events indicating malicious activities. Strengthen your Incident Management process to account for these events and effectively address and respond to these events.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0011** Command and Control	**TA0007** Discovery
TA0005 Defense Evasion	**TA0003** Persistence	**TA0006** Credential Access	**TA0008** Lateral Movement
T1190 Exploit Public-Facing Application	**T1078.002** Valid Accounts: Domain Accounts	**T1070** Indicator Removal	**T1110.004** Brute Force: Credential Stuffing
T1562 Impair Defense	**T1087** Account Discovery	**T1090** Proxy	**T1105** Ingress Tool Transfer
T1135 Network Share Discovery	**T1003** OS Credential Dumping	**T1053** Scheduled Task/ Job	**T1083** File and Directory Discovery
T1021.001 Remote Services: Remote Desktop Protocol	**T1505.003** Server Software Component: Web Shell		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	54[.]255[.]89[.]118, 18[.]195[.]61[.]200
File-Path	c:\users\Redacted\documents\everything-1.4.1.1024.x86\everything.exe, c:\programdata\vmware\66.exe, c:\programdata\vmware\certify.exe, c:\programdata\vmware\kerbrute_windows_amd64.exe, c:\programdata\vmware\msvrp.exe, c:\programdata\vmware\nxc.exe, c:\programdata\vmware\adexplorer64.exe, c:\users\Redacted\documents\h\hrsword install.bat, c:\users\Redacted\documents\h\hrsword.exe, c:\Windows\System32\drivers\sysdiag_win10.sys

TYPE	VALUE
SHA256	d3a6ed07bd3b52c62411132d060560f9c0c88ce183851f16b632a99b4d4e7581, 61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1, 95cc0b082fcfc366a7de8030a6325c099d8012533a3234edbdf555df082413c7, d18aa84b7bf0efde9c6b5db2a38ab1ec9484c59c5284c0bd080f5197bf9388b0, f618b09c0908119399d14f80fc868b002b987006f7c76adbcec1ac11b9208940, 95cc0b082fcfc366a7de8030a6325c099d8012533a3234edbdf555df082413c7, e451287843b3927c6046eaabd3e22b929bc1f445eec23a73b1398b115d02e4fb, 1beec8cecd28fdf9f7e0fc5fb9226b360934086ded84f69e3d542d1362e3fdf3, 6ce228240458563d73c1c3cbbd04ef15cb7c5badacc78ce331848f5431b406cc, acb5de5a69c06b7501f86c0522d10fefa9c34776c7535e937e946c6abfc9bbc6
Network	POST /_vti_bin/client.svc/web/GetFolderByServerRelativeUrl('/BusinessDataMetadataCatalog/')/Files/add(url='/BusinessDataMetadataCatalog/BDCMetadata.bdcm, POST /_vti_bin/DelveApi.ashx/config/ghostfile93.aspx

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094

References

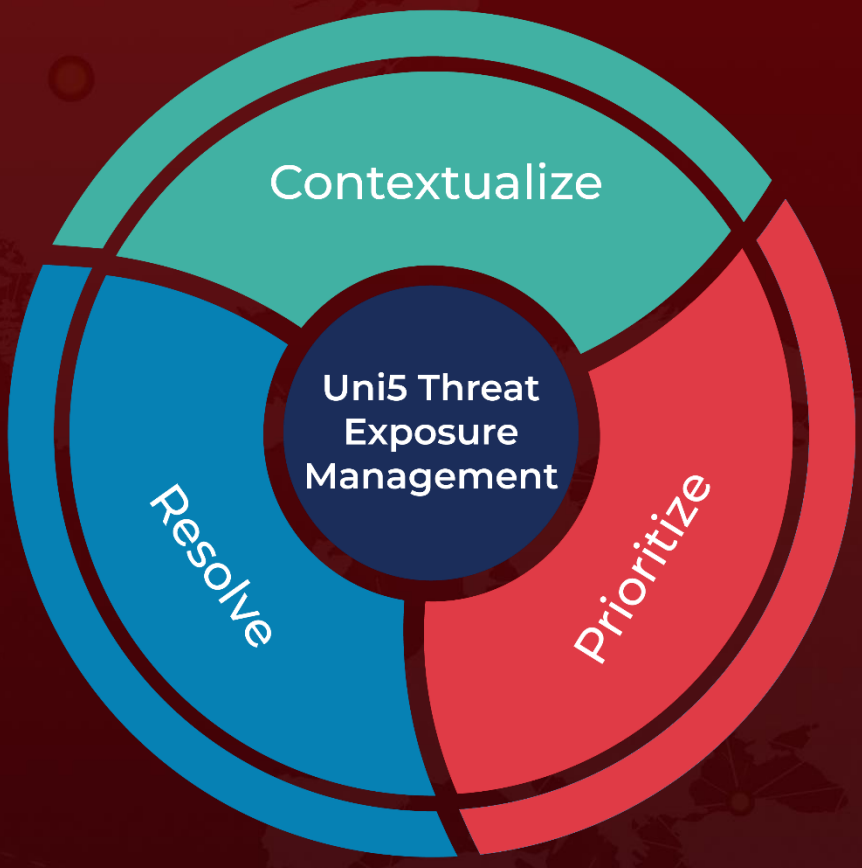
https://www.rapid7.com/blog/post/2024/10/30/investigating-a-sharepoint-compromise-ir-tales-from-the-field/

https://foresiet.com/blog/understanding-sharepoint-remote-code-execution-exploits

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

November 07, 2024 . 01:00 AM

More at www.hivepro.com