CSIS
REST ASSURED

JUNE 27, 2023

MANAGED DETECTION & RESPONSE

Exploitation of CVE-2023-23397 Incident

Microsoft Outlook Elevation of Privilege Vulnerability against customer: detection, analysis, escalation and resolution.

THE POWER OF CSIS'S MDR SERVICE

CSIS detected behavior resembling a recently uncovered exploit discovered in Microsoft Outlook. The exploit needs no user interaction and is triggered when an attacker sends a maliciously formatted Exchange message to user mail accounts. The CSIS MDR Analytics team determined the exact identity and behavior of the exploit. Acting rapidly, the analysts were able to perform full isolation of affected devices and block the malicious IP to prevent further compromise.

THE ATTACKER'S INTENTION

The main objective of the perpetrators was to exploit Outlook using a recently discovered vulnerability to ultimately authenticate against other systems in the organization. To achieve this, the perpetrators sent messages with an extended MAPI property with a UNC path to a SMBshare (TCP 80, 139, and 445) on a threat actor-controlled server. The threat actor then used the connection to the remote SMB server to send the user's NTLM negotiation message, which the attacker can then relay for authentication against other systems that support NTLM authentication within the target organization.

The perpetrators can use privilege escalation attacks to gain privileges they are not entitled to, allowing them to perform any attack they desire, such as: deploying Ransomware/Viruses, exfiltrating confidential data, selling credentials, obtaining further elevated access/lateral movement, etc.

Continued next page…

Continued from previous page...

CSIS IN ACTION

The analyst team quickly detected suspicious activity based on CSIS's constantly evolving detection rules and leveraging Microsoft Defender for Endpoint. CSIS MDR analysts immediately ensured the malicious IP was blocked across the organization and isolated the device.

Applying our expertise in Microsoft Defender, we could determine that there were further exploited machines that Microsoft had yet to catch. The exploited machines were then analyzed and isolated accordingly.

CSIS MDR Team created custom-built Threat Hunting queries to search across the customer's environment for further potential exploits and for connections to the known malicious IP.

The customer was immediately notified through CSIS's proprietary Threat Intelligence Portal and received a Critical Incident Phone Call to their emergency contact.

Having assessed the full capabilities of the attack, CSIS advised the customer to deploy the recently released Microsoft patch for the related CVE to harden their systems against this vulnerability and to execute the Microsoft-provided PowerShell script to scan and clean up their Exchange environment, searching for any further maliciously formatted Exchange messaging items as seen in the CVE (mail, calendar, and tasks). The customer was also provided links to all relevant Microsoft documentation regarding the exploit.

CSIS Analysts took all required actions swiftly, including blocking the IP, crafting advanced custom queries, device identification and isolation, and customer escalation. The customer also quickly cleaned up the affected mailboxes, reset passwords, and patched vulnerable clients.

OUR HIGHLIGHTS

Privilege escalation attacks continue to be prevalent and are a very effective way for cybercriminals to compromise an organization. Privilege escalation attacks can be highly sophisticated and well-designed; the biggest challenge is that an attacker only needs one entry point to initiate a severe, high-impact incident. As this exploit was a relatively recent discovery, many organizations may be vulnerable without knowing their environment is at risk.

To keep systems and user data secure, it is essential that companies ensure the newest patches and security updates are deployed across an organization. Privilege escalation attacks often lead to further compromised systems and exfiltrated, destroyed, or leaked data.

It is also essential to correctly understand the scale and scope of incidents to ensure that remediation actions are comprehensive and effective.

Utilizing our custom detection rules, CSIS rapidly responded and gained a comprehensive interpretation of this attack's scope. Furthermore, by exercising CSIS's analyst expertise, we were able to provide additional value by building custom threat-hunting queries explicitly tailored to this exploit, revealing additional infrastructure compromise.