ITC SECURE

itcsecure.com

Cyber Threat Horizon

Microsoft Outlook Elevation of Privilege

15 March 2023

1 Microsoft Outlook Elevation of Privilege - CVE-2023-23397

CVE-2023-23397 is an elevation of privilege vulnerability in Microsoft Outlook that was assigned a CVSSv3 score of 9.8 with reports that it is activity being exploited in the wild. The vulnerability can be exploited by sending a malicious email to a vulnerable version of Outlook with an extended MAPI property with a UNC path to an SMB (TCP 445) share on a threat actor-controlled server.

When the email is processed by the server, a connection to an attacker-controlled device can be established in order to leak the Net-NTLMv2 hash of the email recipient. The attacker can use this hash to authenticate as the victim recipient in an NTLM relay attack. Microsoft notes that this exploitation can occur before the email is viewed in the preview pane, meaning no interaction from the victim recipient is needed for a successful attack.

ITC-TI analyst comment:

CVE-2023-23397

- ITC recommends patching CVE-2023-23397 which should be picked up in the patching cycle to mitigate this vulnerability. If patching is not immediately possible, ITC recommends the following:
- Add users to the Protected Users group, which prevents the use of NTLM as an authentication mechanism. The Protected Users group provides credential protections beyond disabling NTLM and should be used for high-value accounts, such as domain administrators, when possible.
- Block TCP 445/SMB outbound from your network by using a perimeter firewall, local firewall, and through your VPN settings. For remote users, it is important to check split tunnel VPN settings to ensure outbound traffic is blocked when they are not on your corporate network.

Source: CVE-2023-23397 - Security Update Guide - Microsoft - Microsoft Outlook Elevation of Privilege Vulnerability