CVE-2023-23397 Microsoft Mitigates Outlook Elevation of Privilege Vulnerability

2023-03-15 - Steef | ESET Nederland - Comments (0) - Customer Advisories

Updated Mitigation section - 16-3-2023 14:00

ISSUE

Microsoft Threat Intelligence discovered limited, targeted abuse of a vulnerability in Microsoft Outlook for Windows that allows for new technology LAN manager (NTLM) credential theft. Microsoft has released CVE-2023-23397 to address the critical elevation of privilege (EoP) vulnerability affecting Microsoft Outlook for Windows.
We strongly recommend all customers update Microsoft Outlook for Windows to remain secure.

SOLUTION

Patch

All outlook clients are effected, please patch the clients A.S.A.P. -
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

Mitigate (updated on 16-3-203)

The guidance below provides an additional mitigation which can reduce the risk of WebDAV based attacks until the updated versions can be applied.

Customers can disable the WebClient service running on their organizations machines, similar to our recommendation of blocking TCP/445 traffic.

NOTE: This will block all WebDAV connections including intranet which may impact your users or applications.

The following mitigating factors may be helpful in your situation:

- Add users to the Protected Users Security Group, which prevents the use of NTLM as an authentication mechanism. Performing this mitigation makes troubleshooting easier than other methods of disabling NTLM. Consider using it for high value accounts such as Domain Admins when possible. Please note: This may cause impact to applications that require NTLM, however the settings will revert once the user is removed from the Protected Users Group. Please see Protected Users Security Group for more information.

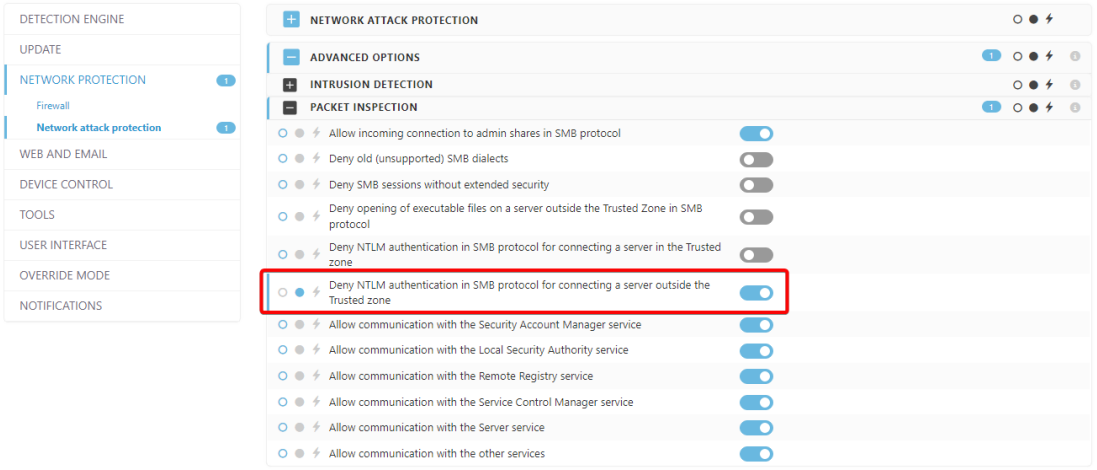
- Block TCP 445/SMB outbound from your network by using a perimeter firewall, a local firewall, and via your VPN settings. This will prevent the sending of NTLM authentication messages to remote file shares.

What can ESET do?

In ESET Endpoint Security (unfortunataly Endpoint Antivirus and Server Security do not have this setting because of firewall dependencies) you can configure the trusted zone for your organisation (via policy or local settings, NETWORK PROTECTION - Zones - edit):

Define your tusted zone using the folowing example/syntax:

With the trusted zone configured, set the following setting: Deny NTLM authentication from outside the trusted zone (via a policy or local settings, NETWORK PROTECTION - Network attack protection - Advanced options - Packet Inspection - Deny NTLM authentication in SMB protocol for connecting a server outside the trusted zone)



Investigate Exchange on premise

To determine if your organization was targeted by actors attempting to use this vulnerability, Microsoft is providing documentation and a script at https://aka.ms/CVE-2023-23397ScriptDoc.

Organizations should review the output of this script to determine risk. Tasks, email messages and calendar items that are detected and point to an unrecognized share should be reviewed to determine if they are malicious. If objects are detected, they should be removed or clear the parameter.

If no objects are detected, it is unlikely the organization was targeted via CVE-2023-23397.