

ESET Tech Center

News > Customer Advisories > CVE-2023-23397 Microsoft Mitigates Outlook Elevation of Privilege Vulnerability

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.

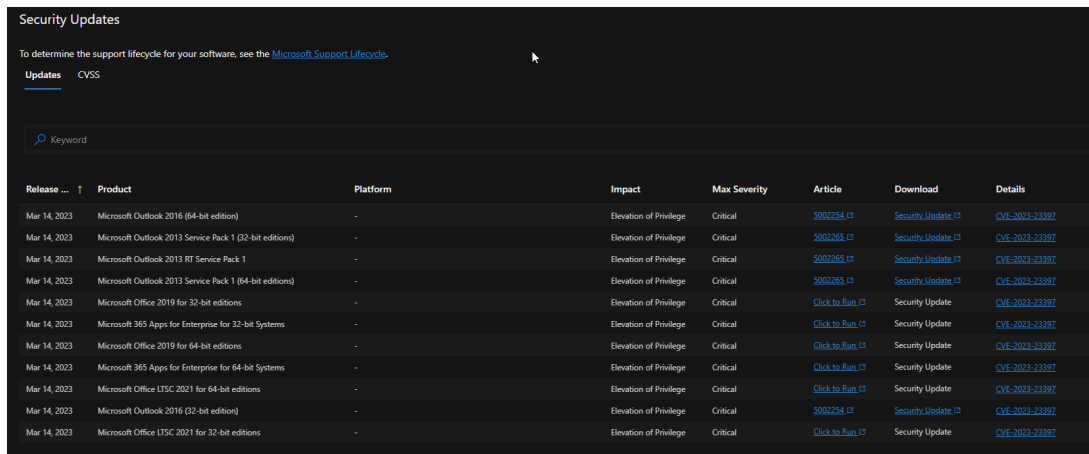
We strongly recommend all customers update Microsoft Outlook for Windows to remain secure.

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>



The screenshot shows the Microsoft Security Updates website. At the top, it says "Security Updates" and "To determine the support lifecycle for your software, see the [Microsoft Support Lifecycle](#)." Below this, there are tabs for "Updates" and "CVSS". A search bar with the placeholder "Keyword" is visible. The main content is a table listing security updates. The table has columns for Release date, Product, Platform, Impact, Max Severity, Article, Download, and Details. The table lists several updates for CVE-2023-23397, all with a "Critical" severity and "Elevation of Privilege" impact. The updates are for Microsoft Outlook 2016 (64-bit edition), Microsoft Outlook 2013 Service Pack 1 (32-bit editions), Microsoft Outlook 2013 RT Service Pack 1, Microsoft Outlook 2013 Service Pack 1 (64-bit editions), Microsoft Office 2019 for 32-bit editions, Microsoft 365 Apps for Enterprise for 32-bit Systems, Microsoft Office 2019 for 64-bit editions, Microsoft 365 Apps for Enterprise for 64-bit Systems, Microsoft Office LTSC 2021 for 64-bit editions, Microsoft Outlook 2016 (32-bit edition), and Microsoft Office LTSC 2021 for 32-bit editions.

Release ... ↑	Product	Platform	Impact	Max Severity	Article	Download	Details
Mar 14, 2023	Microsoft Outlook 2016 (64-bit edition)	-	Elevation of Privilege	Critical	5002254 ⓘ	Security Update ⓘ	CVE-2023-23397
Mar 14, 2023	Microsoft Outlook 2013 Service Pack 1 (32-bit editions)	-	Elevation of Privilege	Critical	5002205 ⓘ	Security Update ⓘ	CVE-2023-23397
Mar 14, 2023	Microsoft Outlook 2013 RT Service Pack 1	-	Elevation of Privilege	Critical	5002265 ⓘ	Security Update ⓘ	CVE-2023-23397
Mar 14, 2023	Microsoft Outlook 2013 Service Pack 1 (64-bit editions)	-	Elevation of Privilege	Critical	5002265 ⓘ	Security Update ⓘ	CVE-2023-23397
Mar 14, 2023	Microsoft Office 2019 for 32-bit editions	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397
Mar 14, 2023	Microsoft 365 Apps for Enterprise for 32-bit Systems	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397
Mar 14, 2023	Microsoft Office 2019 for 64-bit editions	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397
Mar 14, 2023	Microsoft 365 Apps for Enterprise for 64-bit Systems	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397
Mar 14, 2023	Microsoft Office LTSC 2021 for 64-bit editions	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397
Mar 14, 2023	Microsoft Outlook 2016 (32-bit edition)	-	Elevation of Privilege	Critical	5002254 ⓘ	Security Update ⓘ	CVE-2023-23397
Mar 14, 2023	Microsoft Office LTSC 2021 for 32-bit editions	-	Elevation of Privilege	Critical	Click to Run ⓘ	Security Update	CVE-2023-23397

Mitigate (updated on 16-3-2023)

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.

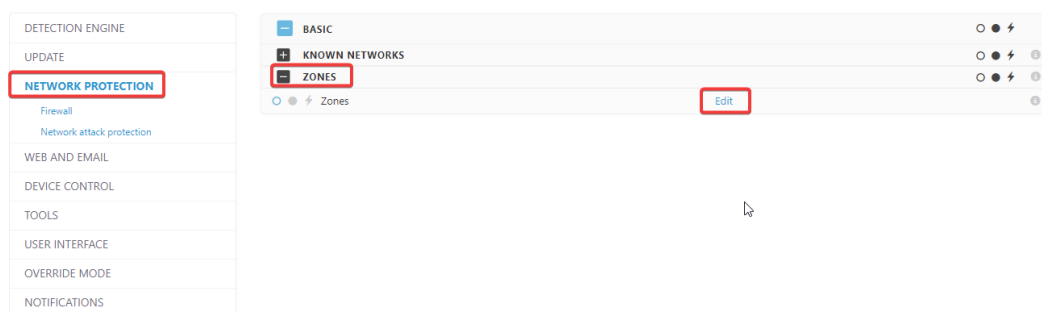
****NOTE:****This will block all WebDAV connections including intranet which may impact your users or applications.

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?

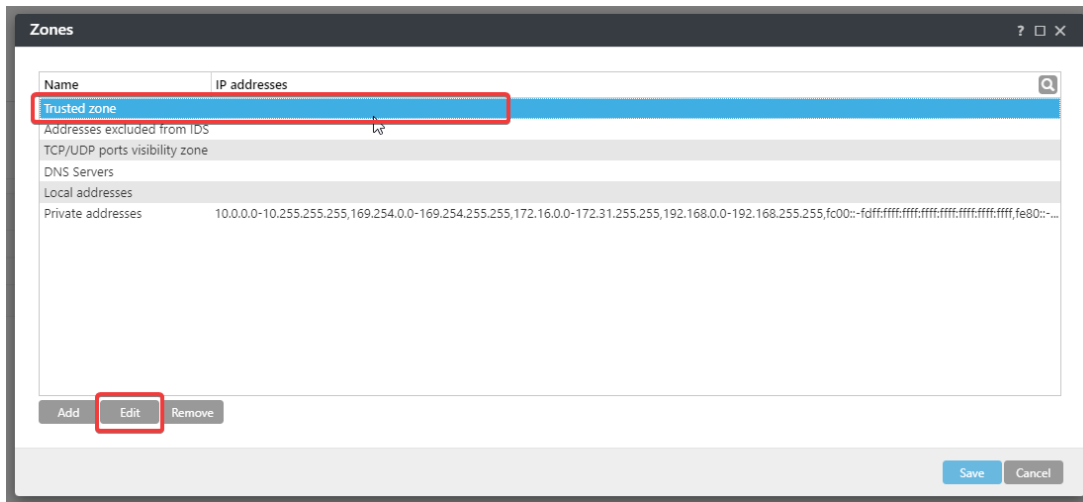
In ESET Endpoint Security (unfortunatly Endpoint Antivirus and Server Security do not have this setting because of firewall dependencies) you can configure the trusted zone for your organisation (via policy or local settings, NETWORK PROTECTION - Zones - edit):



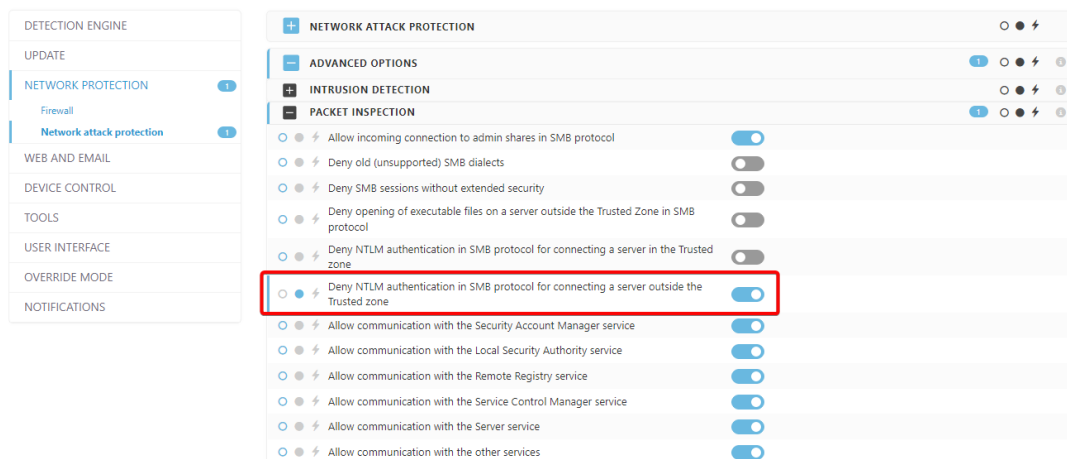
Define your trusted zone using the following example/syntax:

A list of IP addresses or subnets. Multiple entries must be delimited by a comma.

Example: 192.168.1.5, 10.1.0.25-10.1.0.99, 10.1.0.0/255.255.0.0, 10.2.0.0/16, ::1, fe80::/64



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.