

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **New Windows Themes Vulnerability Exposes NTLM Credentials**

Date of Publication

October 30, 2024

Admiralty Code

A1

TA Number

TA2024418










# Summary

**First Seen:** October 29, 2024

**Affected Product:** Microsoft Windows

**Impact:** A new vulnerability in Windows Themes lets attackers steal NTLM credentials by using malicious theme files that require minimal user interaction. It affects fully updated Windows systems from Windows 7 to Windows 11 24H2, making credential theft possible simply by opening the file in Explorer. No official patch is available yet, so users are recommended to implement mitigation measures, such as blocking NTLM hashes via group policy settings.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
Unassigned	Microsoft Windows Themes Spoofing Vulnerability	Microsoft Windows			
CVE-2024-38030	Microsoft Windows Themes Spoofing Vulnerability	Microsoft Windows			
CVE-2024-21320	Microsoft Windows Themes Spoofing Vulnerability	Microsoft Windows			

# Vulnerability Details

## #1

A new vulnerability affecting Windows Themes has been identified, allowing attackers to remotely steal NTLM(New Technology LAN Manager) credentials. NTLM credentials are a type of login information that can be used to access various resources on a network. This vulnerability, which has not yet been assigned a CVE ID, was discovered by a security researcher while developing a micropatch for another related issue (CVE-2024-38030) that could leak user credentials.

## #2

The flaw enables attackers to exploit malicious theme files, triggering unauthorized NTLM authentication requests simply by viewing the file in Windows Explorer. This allows for potential credential theft without any user interaction beyond viewing the theme file.

## #3

The vulnerability impacts all fully updated Windows versions, including Windows 7 through Windows 11 24H2. It is particularly concerning as it can facilitate NTLM relay and pass-the-hash attacks, where attackers use stolen credentials to gain unauthorized access to systems. This discovery follows related issues, including CVE-2024-21320 and CVE-2024-38030, which Microsoft previously patched, but gaps remain that can be exploited.

## #4

Unofficial security patches are available from open-source providers, though they should be applied cautiously and only from trusted sources. Microsoft is aware of the issue and intends to release an official patch soon. In the meantime, they recommend users implement mitigation measures, such as blocking NTLM hashes via group policy settings.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned	Windows: 7 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-200
CVE-2024-38030	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-200
CVE-2024-21320	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-200

# Recommendations



**Stay Updated:** Regularly monitor for security patches from Microsoft, as an official fix is expected. Ensure your Windows operating system is always updated with the latest security patches from Microsoft, as they address known vulnerabilities.



**Disable Themes from Untrusted Sources:** Avoid downloading or applying themes from unknown or unverified sources, as these could contain malicious files that exploit this vulnerability.



**Enable SMB Signing:** Enable SMB signing and use NTLMv2 where possible. SMB signing helps prevent unauthorized users from intercepting credentials during authentication.



**Deploy Endpoint Protection Solutions:** Use comprehensive endpoint protection tools that can detect and block malicious activities related to NTLM credential theft.



**Regular Security Audits:** Perform regular audits of your systems to identify any potential vulnerabilities or unauthorized changes that could lead to security breaches.



## Potential MITRE ATT&CK TTPs

<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>T1204.002</u></b> Malicious File
<b><u>T1204</u></b> User Execution	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.005</u></b> Exploits
<b><u>T1068</u></b> Exploitation for Privilege Escalation			

## Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320>

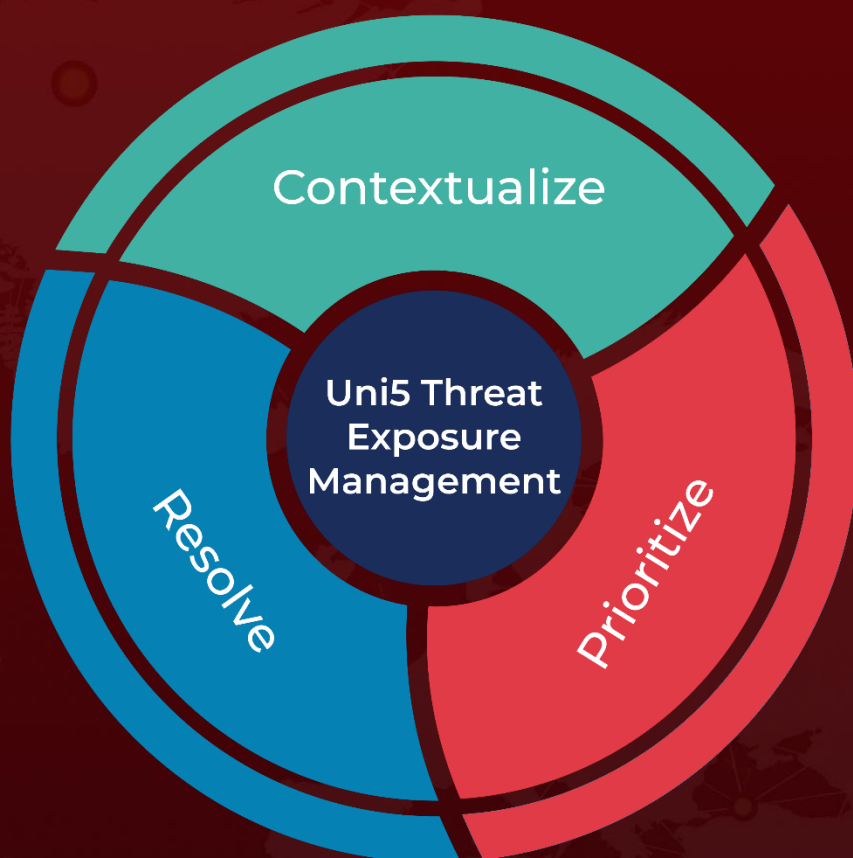
## References

<https://blog.0patch.com/2024/10/we-patched-cve-2024-38030-found-another.html>

# 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

**October 30, 2024 • 7:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)