



Threat Level

 **Amber**

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

'ThemeBleed' flaw in Windows 11 Enables Code Execution

Date of Publication

September 15, 2023

Admiralty Code

A1

TA Number

TA2023374




Summary

First Seen: September 12, 2023

Affected Product: Microsoft Windows Themes

Impact: The CVE-2023-38146 vulnerability in Windows 11 allows remote attackers to execute arbitrary code, potentially compromising the affected system's security and integrity, and posing a significant threat to user data and system functionality.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-38146	Microsoft Windows Themes Remote Code Execution Vulnerability	Microsoft Windows Themes			

Vulnerability Details

#1

CVE-2023-38146, also known as ThemeBleed, presents a significant security risk for Windows 11 users. This high-severity vulnerability was discovered by a security researcher while exploring Windows file formats. It allows remote attackers to execute arbitrary code on a target machine when a user opens a specially crafted .theme file. .theme files are commonly used to customize the appearance of Windows operating systems, making this exploit especially concerning.

#2

The flaw revolves around the handling of .msstyles files and involves a Time-of-Check-Time-of-Use (TOCTOU) issue, creating an opportunity for malicious DLL substitution. Moreover, attackers can evade security warnings by utilizing .themepack files. Microsoft addressed it in the September 2023 update, but some underlying issues remain. Windows 11 users should promptly apply this update for enhanced security.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-38146	Windows 11 version 21H2, Windows 11 version 22H2	cpe:2.3:o:microsoft:windows_11_21h2:*:*:*:*:*:*	CWE-20

Recommendations



Apply the patch: Ensure that the September 2023 Patch Tuesday update or any subsequent security updates addressing the vulnerability are promptly installed on all affected systems running windows11.



Implement Behavior Monitoring: Deploy behavior monitoring tools and security solutions that can detect unusual or malicious behavior on your system. These tools can identify suspicious actions or code execution patterns that may indicate an attack, helping you respond quickly to potential threats. Regularly review and analyze behavior monitoring alerts to stay proactive in identifying and mitigating security risks.



Rogue DLL load Protection: Enable endpoint protection mechanisms to restrict and control DLL loading. This entails permitting only signed and verified DLLs to be loaded into the system.

Potential MITRE ATT&CK TTPs

<u>TA0040</u> Impact	<u>TA0042</u> Resource Development	<u>TA0005</u> Defense Evasion	<u>TA0002</u> Execution
<u>TA0003</u> Persistence	<u>T1574</u> Hijack Execution Flow	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1203</u> Exploitation for Client Execution	<u>T1588.006</u> Vulnerabilities	<u>T1027</u> Obfuscated Files or Information	<u>T1204</u> User Execution
<u>T1574.002</u> DLL Side-Loading			

Patch Link

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146>

References

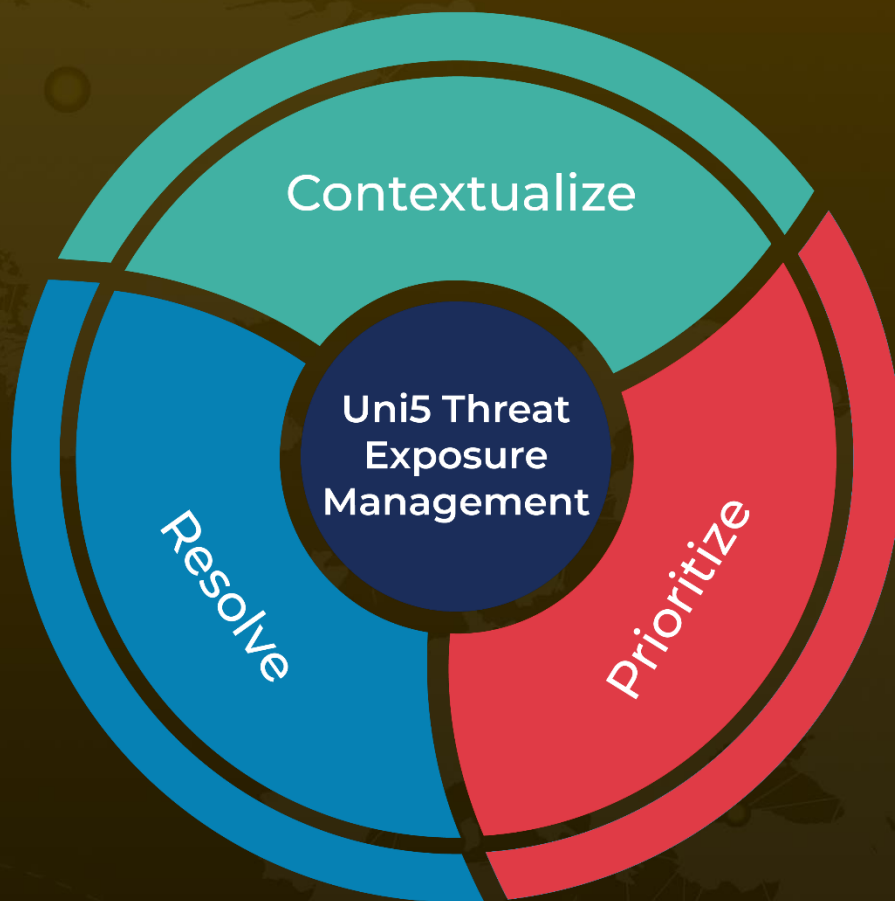
<https://exploits.forsale/themebleed/>

<https://github.com/gabe-k/themebleed>

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

September 15, 2023 • 09:30 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com