

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Windows Zero-Day Vulnerability Exploited by Void Banshee APT

Date of Publication

September 16, 2024

Admiralty Code

A1

TA Number

TA2024357

Summary

First Seen: September 10, 2024







Threat Actor: Void Banshee APT

Malware: Atlantida

Affected Product: Microsoft Windows

Impact: CVE-2024-43461 is a spoofing vulnerability in Microsoft Windows MSHTML, exploited in zero-day attacks by the Void Banshee APT group. It used encoded braille whitespace characters to hide malicious file extensions, making dangerous files appear as harmless PDFs. This enabled the execution of malware, such as the Atlantida info-stealer. Microsoft patched the issue as part of the September 2024 Patch Tuesday updates.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-43461	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows			
CVE-2024-38112	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows			

Vulnerability Details

#1

CVE-2024-43461 is a critical vulnerability in the Windows MSHTML platform, characterized as a spoofing vulnerability. It was disclosed on September 10, 2024, during Microsoft's Patch Tuesday and has a CVSSv3 base score of 8.8, indicating high severity. The vulnerability allows attackers to manipulate the way content is rendered in the MSHTML platform, potentially leading to unauthorized access or execution of malicious code.

#2

Shortly after its disclosure, CVE-2024-43461 was marked as previously exploited in the wild. It was utilized in attacks by the Void Banshee APT group, which targeted organizations to install information-stealing malware. This flaw allowed attackers to manipulate how file extensions appeared to users, making malicious files seem safe to open.

#3

Specifically, it exploited a weakness in how Windows displayed file names, using encoded braille whitespace characters to conceal dangerous file extensions, such as ".hta", behind seemingly harmless ones like ".pdf." When victims opened these disguised files, they would unknowingly execute malicious scripts, often resulting in the download of malware like the Atlantida info-stealer, which targets sensitive data such as passwords and cryptocurrency wallets.

#4

CVE-2024-43461 was part of a broader attack chain, also involving another zero-day ([CVE-2024-38112](#)), which forced Windows to open malicious websites via Internet Explorer. Microsoft patched CVE-2024-43461 in their September 2024 updates, ensuring that braille whitespace characters no longer obscure file extensions, thus exposing the file's true nature.

#5

Given its critical nature and the fact that it has already been exploited in attacks, and its ability to facilitate unauthorized actions on affected systems, immediate action is recommended for all supported versions of Windows.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-43461	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *.*	CWE-451
CVE-2024-38112	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *.*	CWE-451

Recommendations



Apply Patches and Updates: Ensure that all Windows systems are updated with the latest security patches released by Microsoft. This is the most effective way to mitigate the vulnerability. Establish a routine for checking and applying updates to ensure that all systems remain secure against known vulnerabilities.



Strengthen File Execution Policies: Restrict execution of potentially dangerous file types, such as .hta and .exe, especially from untrusted sources. This can help prevent malicious scripts from running even if they bypass detection methods.



Enhance User Awareness: Conduct regular security awareness training, emphasizing the dangers of opening email attachments or files from untrusted sources. Teach users to check file extensions carefully and avoid files that appear suspicious, even if they seem like PDFs or other legitimate formats.



Improve Email and Web Filtering: Deploy robust email filtering solutions to block phishing attempts and malicious attachments. Advanced filtering mechanisms can prevent delivery of spoofed or deceptive files that exploit such vulnerabilities.

Potential MITRE ATT&CK TTPs

<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0005</u> Defense Evasion	<u>TA0002</u> Execution
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1204</u> User Execution	<u>T1204.002</u> Malicious File	<u>T1036</u> Masquerading	<u>T1059</u> Command and Scripting Interpreter
<u>T1587.001</u> Malware	<u>T1587</u> Develop Capabilities		

Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112>

References

<https://www.bleepingcomputer.com/news/security/windows-vulnerability-abused-braille-spaces-in-zero-day-attacks/>

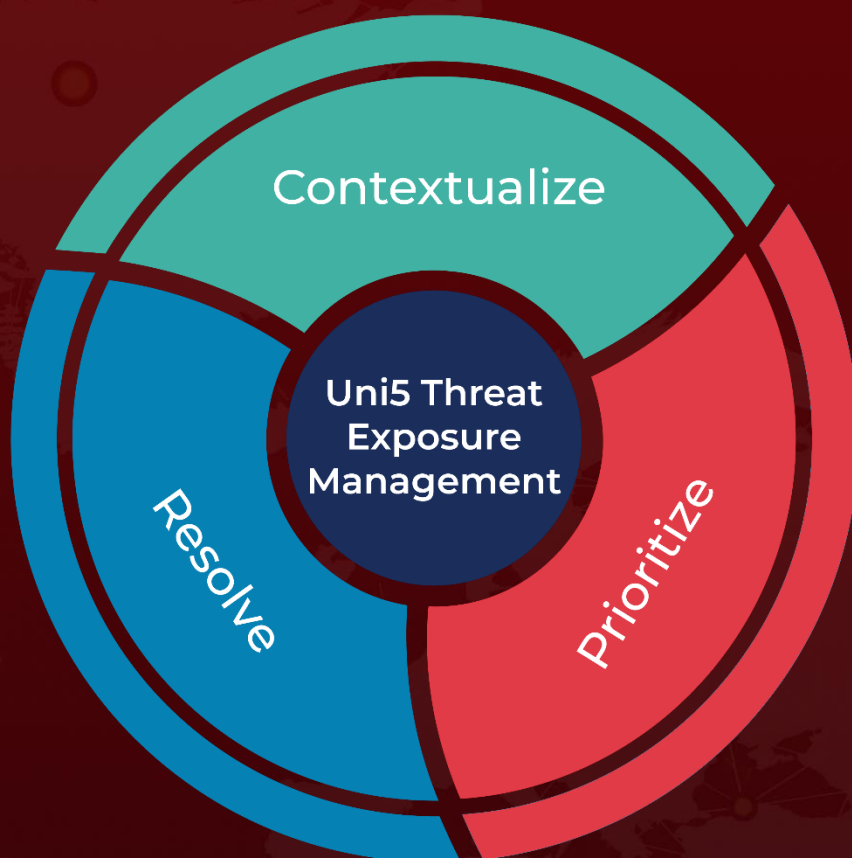
<https://hivepro.com/threat-advisory/void-banshees-zero-day-assault-on-windows-users-via-internet-explorer/>

<https://hivepro.com/threat-advisory/microsofts-september-patch-tuesday-addresses-active-zero-day-exploits/>

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 16, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com