

Hiveforce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

A Flaw in Microsoft Visual Studio Installer Enables Malicious Extension Distribution

Date of Publication

June 13, 2023

Admiralty Code

A1

TA Number

TA2023260




Summary

First Seen: April 11, 2023

Affected Product: Microsoft Visual Studio

Impact: The vulnerability allows attackers to gain unauthorized access, compromise systems, and distribute malicious extensions, posing a significant security risk.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-28299	Visual Studio Spoofing Vulnerability	Microsoft Visual Studio			

Vulnerability Details

#1

A vulnerability in the Microsoft Visual Studio installer, known as CVE-2023-28299, allowed malicious actors to distribute and install fake extensions by spoofing publisher digital signatures. This vulnerability was addressed by Microsoft in April 2023. By adding newline characters to the extension's name, the warning about the extension not being digitally signed could be hidden, tricking developers into installing the malicious extension.

#2

Attackers could exploit this by sending phishing emails with the spoofed extension or attaching malicious VSIX files, gaining unauthorized access to targeted systems and potentially compromising networks, and stealing sensitive information. Microsoft released a patch to fix the vulnerability, and users are advised to apply the patch and remain vigilant for suspicious activity.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28299	Visual Studio: 2017 version 15.9; 2022 version 17.4, 17.4, 17.2, 17.0; 2019 version 16.11	cpe:2.3:a:microsoft:visual_studio_2017:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2019:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:*	CWE-451

Recommendations



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



Exercise caution with email attachments: Be cautious when opening email attachments, particularly those claiming to be software updates. Verify the sender's authenticity and the legitimacy of the attachment before downloading or executing any files.



Educate and raise awareness: Provide comprehensive training to developers and users about the risks associated with phishing emails and the installation of untrusted extensions. Promote best practices for identifying suspicious emails and emphasize the importance of vigilant behavior when installing software or extensions.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0010</u> Exfiltration	<u>TA0011</u> Command and Control	<u>TA0009</u> Collection
<u>TA0007</u> Discovery	<u>TA0040</u> Impact	<u>TA0005</u> Defense Evasion	<u>TA0002</u> Execution
<u>T1036</u> Masquerading	<u>T1566</u> Phishing	<u>T1566.001</u> Spearphishing Attachment	<u>T1218</u> System Binary Proxy Execution
<u>T1005</u> Data from Local System	<u>T1204.002</u> Malicious File	<u>T1204</u> User Execution	<u>T1082</u> System Information Discovery
<u>T1021</u> Remote Services	<u>T1485</u> Data Destruction		

Patch Link

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28299>

References

<https://twitter.com/SamSays47/status/1668499053007732737>

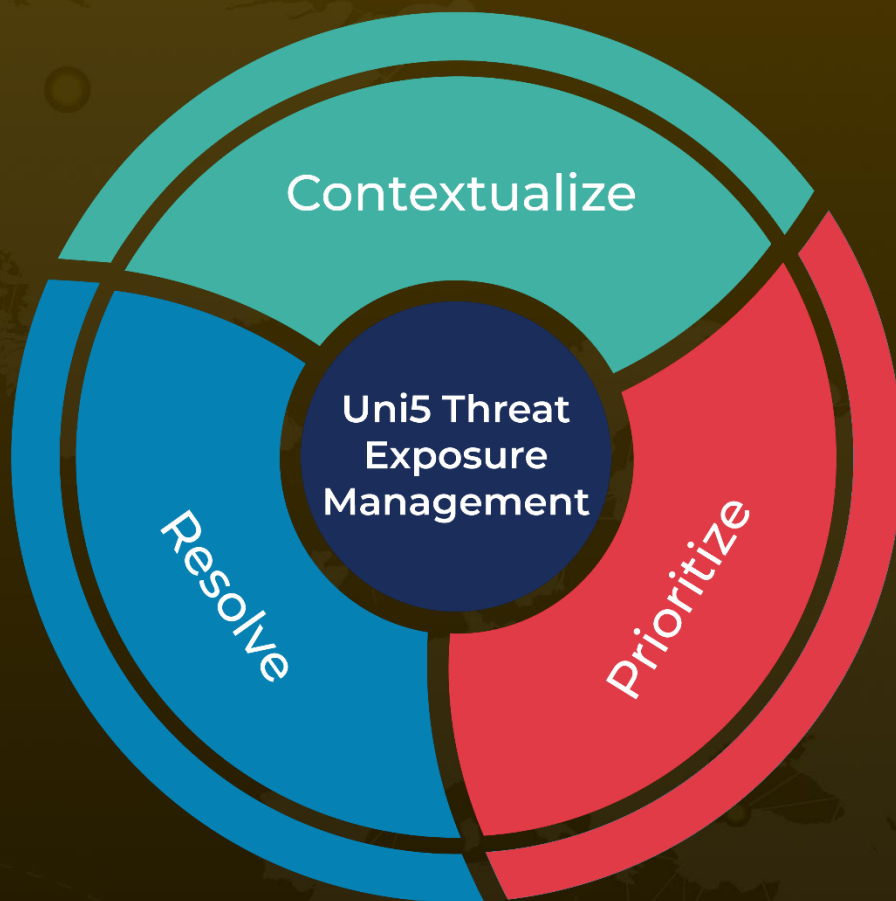
<https://thehackernews.com/2023/06/researchers-uncover-publisher-spoofing.html?m=1>

<https://www.varonis.com/blog/visual-studio-bug>

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

June 13, 2023 • 03:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com