

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Trend Micro Addresses Zero-Day Flaws Exploited in the Wild

Date of Publication

September 20, 2023

Admiralty Code

A1

TA Number

TA2023377

Summary




First Seen: September 19, 2023

Affected Products: Apex One and Worry-Free Business Security

Affected Platform: Windows

Impact: A critical zero-day vulnerability, tracked as CVE-2023-41179, has been identified in the third-party AV uninstaller module contained in Trend Micro Apex One, Worry-Free Business Security, and Worry-Free Business Security Services. This vulnerability has the potential to allow an attacker to manipulate the module and execute arbitrary commands on an affected installation. This is a serious security issue that can lead to unauthorized code execution with system privileges on deployed agents.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-41179	Trend Micro Arbitrary Code Execution Vulnerability	Apex One and Worry-Free Business Security			

Vulnerability Details

#1

The arbitrary code execution flaw, identified as CVE-2023-41179, impacts several Trend Micro security products, including Apex One, Apex One SaaS, and Worry-Free Business Security. This vulnerability is related to a third-party uninstaller module that is included with these security software products.

#2

This security flaw arises from inadequate input validation within the third-party antivirus (AV) uninstaller module that is bundled with the software. If the vulnerability is successfully exploited, an attacker who has access to the product's administration console can potentially execute arbitrary code with system-level privileges on the computer where the security agent is installed. This represents a significant security risk, as it could allow an attacker to gain full control over the compromised system.




#3

The fact that this vulnerability has been exploited in the wild underscores the urgency of addressing the issue promptly. Organizations using Trend Micro's affected products, such as Apex One, Apex One SaaS, or Worry-Free Business Security, should take immediate action to update to the latest version.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-41179	Trend Micro Apex One On Premise (2019) Trend Micro Apex One as a Service Worry-Free Business Security 10.0 SP1 Worry-Free Business Security Services (SaaS)	cpe:2.3:a:trend_micro:apex_one:CP_12033:*:*:*:*:*	CWE-78

Recommendations

-  **Apply Patch:** Install the security patch provided by Trend Micro to address the CVE-2023-41179 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.
-  **Least privilege:** Adhere to the idea of least privilege by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.
-  **Access Control:** Limiting access to the product's admin console to trusted networks is a practical way to boost security. It reduces the attack surface and lowers the risk of unauthorized external access.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation
<u>T1587.004</u> Exploits	<u>T1203</u> Exploitation for Client Execution	<u>T1587</u> Develop Capabilities	<u>T1068</u> Exploitation for Privilege Escalation

Patch Link

Apply the Following Firmware Updates:

Apex One 2019 Service Pack 1 – Patch 1 (Build 12380)

Apex One SaaS 14.0.12637

WFBS Patch 2495

WFBSS July 31 update

<https://success.trendmicro.com/dcx/s/solution/000294994/>

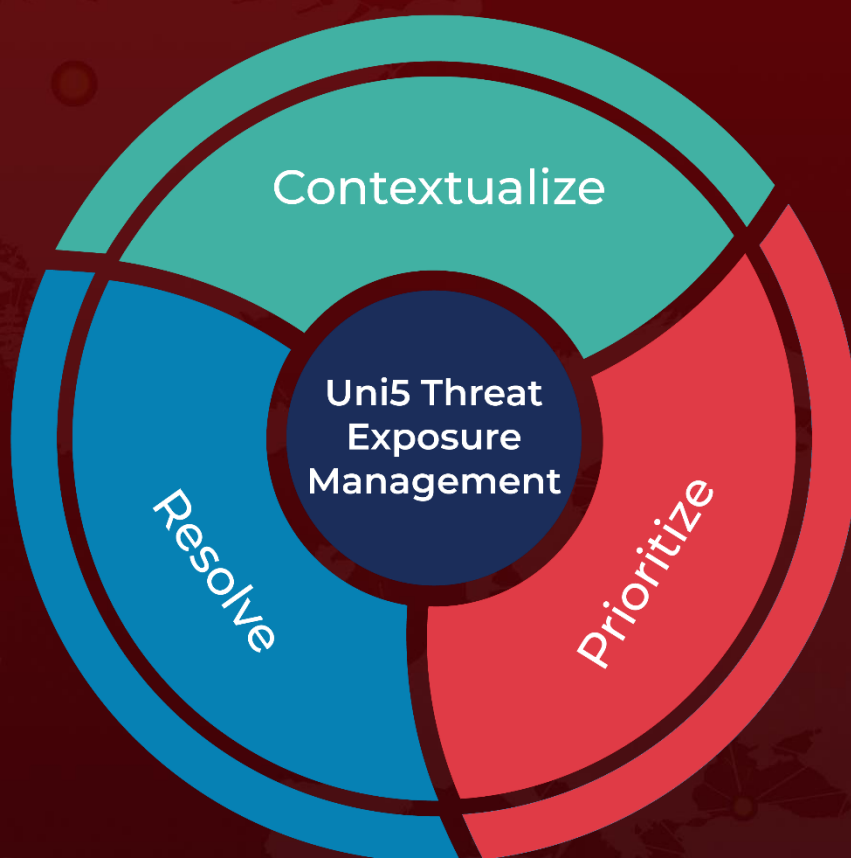
References

<https://www.jpCERT.or.jp/english/at/2023/at230021.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

September 20, 2023 • 6:10 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com