Hive Pro

THREAT ADVISORY

Actively exploited vulnerability affects Trend Micro Apex Central

TA2022086

Threat Level AMBER

Publish Date – April 1, 2022

Trend Micro Apex Central (on-premise and as a Service) has a zero-day vulnerability This arbitrary file upload vulnerability if successfully exploited, could allow an unauthenticated remote attacker to upload any file, resulting in remote code execution. Organizations are advised to upgrade their Apex Central to the latest version available.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
TA0001: Initial Access
TA0002: Execution
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
T1190: Exploit Public-Facing Application
T1059: Command and Scripting Interpreter

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-26871	Trend Micro Apex Central Build: Less than 6016 Trend Micro Apex Central as a Service (SaaS) Build: less than 202203	cpe:2.3:a:trendmicro:apex_central:*:*:*:*:*:*:*:*	Trend Micro Apex Central Arbitrary File Upload Remote Code Execution (RCE) Vulnerability	CWE-345

Patch Links

https://files.trendmicro.com/jp/ucmodule/apexcentral/win/2019/apexcentral_2019_gm_win_ja_3945_r3.exe
https://appweb.trendmicro.com/supportNews/NewsDetail.aspx?id=4395

References

https://success.trendmicro.com/jp/solution/000290660
https://jvn.jp/vu/JVNVU99107357/