Nightmare week for security vendors: Now a Trend Micro bug is being exploited in the wild

therecord.media/nightmare-week-for-security-vendors-now-a-trend-micro-bug-is-being-exploited-in-the-wild/

April 22, 2021

US-Japanese cybersecurity firm Trend Micro disclosed on Wednesday that a threat actor began using a bug in its antivirus products to gain admin rights on Windows systems as part of its attacks.

The vulnerability, tracked as **CVE-2020-24557**, affects the company's Apex One and OfficeScan XG, two advanced security products aimed at enterprise customers.

The bug was discovered last year by Christopher Vella, a vulnerability researcher at Microsoft, who privately reported the issue to Trend Micro through the company's Zero-Day Initiative bug acquisition program.

Trend Micro patched the issue in August 2020, but in an update to its initial security advisory posted on Wednesday, the security firm said it learned of incidents where this same bug was weaponized to attack some of its customers.

"The specific flaw exists within the logic that controls access to the Misc folder," the ZDI team said last year. "An attacker can leverage this vulnerability to escalate privileges and execute code in the context of SYSTEM."

Based on this description of the issue, the bug could not be used to break into systems but was used as a second step in a multi-phase exploit chain after hackers already planted malicious code on a victim's computer and used the bug to take full control of an infected system.

While Trend Micro did not share any details about the attackers, a source familiar with the attacks told *The Record* the bug was used by an advanced persistent threat (APT), a term usually used to refer to state-sponsored cyber-espionage groups.

This bug now becomes the fourth vulnerability in Apex One and OfficeScan XG security products that has been exploited in the wild after CVE-2019-18187, CVE-2020-8467, and CVE-2020-8468.

The first three were abused in 2019 and 2020, with the first being used by a Chinese cyber-espionage group during an attack on Mitsubishi Electric.

A bad week for security product vendors

News about hackers exploiting the Trend Micro vulnerability comes a day after FireEye disclosed that multiple hacking groups had also exploited zero-day in security products from Pulse Secure and SonicWall.

While all these attacks are unrelated, they show a pattern in real-world attacks where threat actors are slowly realizing that security products are as vulnerable as any other software, and, because of the central and privileged position they occupy inside most corporate networks, they are ideal entry points into high-profile targets.

Tags

- antivirus
- exploit
- Office
- security software
- Trend Micro

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.