Alert Bulletin

Bulletin N.: 2023-01

Publication Date: 16/11/2023

Subject: Alert 2023-01 – Active Exploitation of Critical Vulnerability in Trend Micro Products

Traffic Light Protocol (TLP): White

A critical vulnerability affecting Trend Micro products has been reported as CVE-2023-41179 classified as critical with a CVSS score of 7.2. The vulnerability specifically affects the AV uninstall module (developed by a third party), which is contained in Trend Micro Apex One (on-premises and SaaS), Worry-Free Business Security and Worry-Free Business Security Services. There are indications that this vulnerability is currently being actively exploited. Exploitation of this vulnerability could allow an attacker to manipulate the module to execute arbitrary commands on an affected site. It is important to note that an attacker must first gain access to the administrative console on the target system in order to exploit this vulnerability. Trend Micro's research team, mentioned in its report, that "Trend Micro has detected at least one instance of a possible exploit attempt of CVE-2023- 41179." It also emphasized that "although the exploit may require the fulfillment of several specific conditions, Trend Micro strongly recommends that customers upgrade to the latest versions as soon as possible".