CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-016

Multiple Critical Vulnerabilities in Trend Micro

March 18, 2020 — v1.0

TLP:WHITE

History:

- *18/03/2020 — v1.0 – Initial publication*

Summary

On the 16th of March 2020, Trend Micro has released critical patches for two remote code execution vulnerabilities in **Trend Micro Apex One** and **OfficeScan XG** along with other three critical vulnerabilities [1]. Trend Micro confirmed that they identified active attempts against the zero-day vulnerabilities, but without disclosing more details.

It is strongly recommended to update, especially because exploits are available and there were attack attempts. Even if the zero-days require user authentication, they could be used in a post-compromise scenario to either disable the security products or elevate the attackers' privileges on machines running the two Trend Micro antivirus products [2].

Technical Details

The vulnerability CVE-2020-8467 with **critical severity** (CVSSv3 score of 9.1) is due to a migration tool component of Trend Micro Apex One and OfficeScan that contains a vulnerability which could allow remote attackers to execute arbitrary code on affected installations (RCE). An attempted attack requires user authentication.

The vulnerability CVE-2020-8468 with **high severity** (CVSSv3 score of 8.0) is due to the Trend Micro Apex One and OfficeScan agents that are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.

The vulnerability CVE-2020-8470 with **critical severity** (CVSSv3 score of 10) is due to the Trend Micro Apex One and OfficeScan server which contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.

The vulnerability CVE-2020-8598 with **critical severity** (CVSSv3 score of 10) is due to the Trend Micro Apex One and OfficeScan server which contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.

The vulnerability CVE-2020-8599 with **critical severity** (CVSSv3 score of 10) is due to the Trend Micro Apex One and OfficeScan server which contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this vulnerability.

Products Affected

Products affected by the critical and high severity vulnerabilities:

- Apex One (on premise) version 2019 Platform: Windows
- OfficeScan versions XG SP1 and XG (non-SP) Platform: Windows

Recommendations

Update Trend Micro products to the latest versions:

- Apex One (on premise) CP 2117
- OfficeScan XG SP1 CP 5474
- OfficeScan XG CP 1988

References

[1] https://success.trendmicro.com/solution/000245571

[2] https://www.zdnet.com/article/two-trend-micro-zero-days-exploited-in-the-wild-by-hackers/