The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/31/2022

SUBJECT:
A Vulnerability in Trend Micro Apex Central Could Allow for Arbitrary File Upload

OVERVIEW:
A vulnerability has been discovered in Trend Micro Apex Central which could allow for arbitrary file upload. Trend Micro Apex Central is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Successful exploitation of this vulnerability could result in arbitrary file upload which could allow a remote attacker to execute arbitrary code. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
Trend Micro has observed an active attempt of exploitation against this vulnerability in-the-wild (ITW) in a very limited number of instances.

SYSTEMS AFFECTED:

- Apex Central (on-prem) versions before Patch 3 (Build 6016)
- Apex Central (SaaS) versions before the March 9, 2022 Deployment (Build 6016)

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Trend Micro Apex Central which could allow for arbitrary file upload.

Successful exploitation of this vulnerability could allow an unauthorized attacker to upload arbitrary files, possibly leading to remote code execution. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Trend Micro to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Trend Micro:
https://success.trendmicro.com/dcx/s/solution/000290678?language=en_US

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26871