Severity

High

Analysis Summary

CVE-2022-28394 CVSS:7.8

Trend Micro Password Manager could allow a remote attacker to execute arbitrary code on the system, caused by improper loading of dynamic link libraries in the installer. By persuading a victim to use a specially-crafted DLL file, an attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the user who invoked the installer.

Impact

- Code Execution

Indicators Of Compromise

CVE

- CVE-2022-29108

Affected Vendors

- Trend Micro

Affected Products

Trend Micro Password Manager 3.7.0.0 Trend Micro Password Manager 3.6.0.0

Remediation

Refer to Trend Micro Security Advisory for patch, upgrade or suggested workaround information.

Trend Micro Security Advisory