Severity

High

Analysis Summary

CVE-2022-30523

Trend Micro Password Manager could allow a local authenticated attacker to gain elevated privileges on the system, caused by a link following vulnerability. By creating a symbolic link, an attacker could exploit this vulnerability to abuse the service to delete a file and execute arbitrary code with SYSTEM privileges.

Impact

- Privilege Escalation

Indicators Of Compromise

CVE

- CVE-2022-30523

Affected Vendors

- Trend Micro

Affected Products

Trend Micro Password Manager 5.0.0.1266

Remediation

Refer to Trend Micro Web site for patch, upgrade or suggested workaround information.

Trend Micro Website