Severity

High

Analysis Summary

CVE-2022-28339

This vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro HouseCall for Home Networks. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.

The specific flaw exists within the log4j scanner. The process loads a file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of an administrator.

Impact

Privilege Escalation

Indicators Of Compromise

CVE

CVE-2022-28339

Affected Vendors

Trend Micro

Affected Products

HouseCall for Home Networks

Remediation

For patches, updates, and workarounds refer to the following vendor website:

Trend Micro