مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in Trend Micro Deep Security 20 Agent
Tracking #:432316531
Date:20-11-2024

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Trend Micro has issued a security update for the Trend Micro Deep Security 20 Agent and Deep Security Notifier on DSVA to address a remote code execution (RCE) vulnerability.

TECHNICAL DETAILS:

Trend Micro has issued a security update for the Trend Micro Deep Security 20 Agent and Deep Security Notifier on DSVA to address a remote code execution (RCE) vulnerability identified as CVE-2024-51503. This vulnerability stems from a manual scan command injection flaw, which could allow attackers to escalate privileges and execute arbitrary code on affected system.

Vulnerability Details:
- **CVE Identifier**: CVE-2024-51503
- **Vulnerability Type**: OS Command Injection (Manual Scan)
- **CVSS v3.0 Score**: 8.0 (High)
- A security agent manual scan command injection vulnerability in the Trend Micro Deep Security 20 Agent could allow an attacker to escalate privileges and execute arbitrary code on an affected machine. In certain circumstances, attackers that have legitimate access to the domain may be able to remotely inject commands to other machines in the same domain.
- **Vulnerable Product(s):**
  o Deep Security Agent: Versions prior to 20.0.1-21510
  o Deep Security Notifier on DSVA: Version 20.0.0-8438 only
- **Platform:** Windows
- **Fixed Versions:**
  o Deep Security Agent: 20.0.1-21510 or higher
  o Deep Security Notifier on DSVA DSA - Affected clients should install DSA 20.0.1 full package

RECOMMENDATIONS:

- Install the latest available version and apply patches as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://success.trendmicro.com/en-US/solution/KA-0018154