Local Privilege Escalation through Trend Micro OfficeScan

Published Date	07/08/2015
Vendor	Trend Micro
Product	OfficeScan
Affected Versions	11.1 and earlier
Vendor Advisory	http://esupport.trendmicro.com/solution/en-US/1110988.aspx
CVSS	6.8
CVE Reference	*TBA*
Author/s	Andrew Kitis, Sagi Shahar, David Taylor

Description

A local privilege escalation vulnerability was found in Trend Micro's OfficeScan product when the 'Normal' security level is chosen during product installation. This vulnerability allows an attacker, with unprivileged access to an affected system to escalate their privileges to that of a local administrator.

This vulnerability is similar to the previously reported privilege escalation vulnerability within OfficeScan, CVE-2006-1381.

Cause

When OfficeScan is installed with 'Normal' security level, the filesystem permissions on the installation folder (and all files and sub-folders within) are set such that "Everyone" has "Full Control". (Note: 'Normal' is not the default security level setting).

After installation, several OfficeScan services are created, running as SYSTEM, based on executables that exist within the OfficeScan installation folder.

An attacker can overwrite one of these service executables with malicious executable content, then force the malicious code to be executed by rebooting the Windows system.

Impact

An attacker with unprivileged access to an affected system can execute arbitrary code on the system, with the privileges of SYSTEM.

Solution

Trend Micro have published an advisory with a solution.

Technical Details

To exploit this vulnerability, we took the following steps:

1. Reboot the Windows system into Safe Mode so that the OfficeScan processes are not running.
2. Overwrite the ntrtscan.exe (Real Time Scan Service) executable in the installation directory with a crafted executable. In our instance, the crafted executable created a new local user account and added this to the "Local Administrators" group.
3. Reboot the Windows system. During startup, the Real Time Scan Service executable (ntrtscan.exe) is started, executing the crafted payload.