README.md

CVE_Assessments_02_2020

Product: AutoHotkey version 1.1.32.00

Download: https://www.autohotkey.com/download/ahk-install.exe

The AutoHotkey version 1.1.32.00 is vulnerable to process injection.

The AutoHotkey has one detection using VirusTotal.
https://www.virustotal.com/gui/file/ce505d272f8d36c5599ac81f005e1d2d586eeaaa778c779ad858e44fdadfdb0d/details https://www.hybrid-analysis.com/sample/ce505d272f8d36c5599ac81f005e1d2d586eeaaa778c779ad858e44fdadfdb0d

But If we look closer to some of the names of the file, it refers to a hash with a high level of detection.

Ex: fa0842f2292240e5405af9e2d03177ce40335b3d94e881305ce9b43c1eeb02a8
https://www.virustotal.com/gui/file/fa0842f2292240e5405af9e2d03177ce40335b3d94e881305ce9b43c1eeb02a8/detection

Components: AutoHotkey_1.1.32.00_setup.exe (PID: 3988), setup.exe (PID: 3596).

This is the file used in the injection (setup.exe):
https://www.virustotal.com/gui/file/809cde49325a1834ac63ba879d1e751f80086d0ac5a5b3b096cf8257ca2e5531/details

A similar issue was previously observed in older versions of this product: https://www.autohotkey.com/boards/viewtopic.php?t=13985

The problem is likely to be found in the overlay.

Also note that this software uses a ShellExecuteEx which could allow local users to gain privilege (CVE-2014-1807). Security aspects related to this function can be found at:

https://docs.microsoft.com/en-us/windows/win32/shell/sec-shell

https://docs.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecuteexa

Attributes that we can search for associated with the event of an insufficient buffer are:

I. System process connects to network (likely due to code injection or exploit)

II. Modifies the context of a thread in another process (thread injection)

III. Allocates memory in foreign processes

IV. Queues an APC in another process (thread injection)

V. Maps a DLL or memory area into another process

VI. Writes to foreign memory regions

VII. Creates a process in suspended mode (likely to inject code)