MS14-019 – Fixing a binary hijacking via .cmd or .bat file

By swiat

Published: 2014-04-08 · Archived: 2026-04-06 00:03:08 UTC

/ By / April 8, 2014

Command (.cmd) and batch (.bat) files can be directly provided as input to the CreateProcess as if it is an executable. CreateProcess uses the cmd.exe automatically to run the input .cmd or .bat.

Today, with the bulletin MS14-019 we are fixing a vulnerability, where in particular scenario it is possible to hijack the cmd.exe with a copy present in the attacker controlled current working directory (CWD) of an affected application.

The typical attack vector for this vulnerability is same as the DLL hijacking, i.e., via opening an application specific file in a WebDav/SMB share invoking the targeted application automatically because of file association. The targeted application will be vulnerable only if they ever do CreateProcess on .cmd or .bat file irrespective of where the file is located. That means attacker need not control the .cmd or .bat file. Another important thing for exploiting this vulnerability, is that the application should set the directory from where the associated file was opened as its CWD.

As such we are not aware of any application that is affected by this vulnerability. But we understand the security issue this vulnerability can pose to some of the applications, so we are addressing this as an important severity bulletin.

The way we are fixing this issue is to always invoke the system version of the cmd.exe for the input .cmd or .bat file during process creation. This fix could affect applications which does CreateProcess on .bat or .cmd file directly and depend on a different version of the cmd.exe other than the one present in Sytem directory by copying them in either application directory or CWD. Such applications should pass fully qualified path to the version of cmd.exe as input while performing CreateProcess, and pass .cmd or .bat as input parameters.

Applications passing just cmd.exe to the CreateProcess to run the .cmd or .bat as input could also be vulnerable for similar binary hijacking. This bulletin is not to address such vulnerable usage since it is application specific problem as they are not passing fully qualified system path to cmd.exe. Such application should fixed to pass fully qualified cmd.exe path or just passing .cmd or .bat file as input.

- Swamy Shivaganga Nagaraju, MSRC engineering team

- MS14-019 CMD BAT CreateProcess
