CVE-2020-0938 – Score: 7.8

Components:

- microsoft windows 8.1 -
- microsoft windows server 2008 -
- microsoft windows server 2019 -
- microsoft windows server 2008 r2
- microsoft windows server 2012 r2
- microsoft windows 10 1709
- microsoft windows 10 -
- microsoft windows 10 1809
- microsoft windows 10 1909
- microsoft windows server 2016 1909
- microsoft windows 7 -
- microsoft windows 10 1903
- microsoft windows 10 1607
- microsoft windows server 2016 1903
- microsoft windows server 2016 1803
- microsoft windows 10 1803
- microsoft windows server 2012 -
- microsoft windows rt 8.1 -
- microsoft windows server 2016 -

Description:

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.

Main problems:

787 "Out-of-bounds Write"