NVD DB Update

CVE-2020-1380 - Score: 7.8

Components:

microsoft windows 8.1 -
microsoft windows 10 1709 -
microsoft windows 10 1903 -
microsoft windows server 2019 -
microsoft windows server 2008 r2
microsoft windows server 2012 r2
microsoft internet explorer 11
microsoft windows 7 -
microsoft windows 10 1803 -
microsoft windows 10 1607 -
microsoft windows 10 1809 -
microsoft windows 10 1909 -
microsoft windows server 2012 -
microsoft windows 10 1507 -
microsoft windows rt 8.1 -
microsoft windows server 2016 -
microsoft windows 10 2004 -

Description:

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe