Issued 12/12/17

Microsoft Releases Emergency Windows Patch for Flaw in Malware Protection Engine

Microsoft has just published an emergency security update for all supported Windows versions to address a remote code execution (RCE) flaw in the Malware Protection Engine. Documented as CVE - 2017 - 11937, the vulnerability has been confirmed in Windows 7, Windows 8.1, Windows 10, Windows RT 8.1, and Windows Server with Microsoft security software like Windows Defender, Microsoft Security Essentials, Endpoint Protection, and Intune Endpoint Protection.

According to Microsoft, the flaw exists in the way the Malware Protection Engine handles a specially crafted file, as it can be tricked to cause m emory corruption and then provide the attacker with rights to executive arbitrary code on the target system. This could, in the end, provide the attacker with full control of the system, which would basically mean that they get administrator privileges on the computer. A successful exploit means that hackers need to deploy the crafted file on the victim's computer, and this can be done via email, messaging apps, or with links to websites hosting the file, again distributed via various ways.

The update is applied automatically by the Malware Protection Engine, and Microsoft says that its patching mechanism should apply it within 48 hours of release.