Microsoft released an emergency security patch for a serious vulnerability

If you are using Windows OS, install this security patch now.

If you are using Windows OS, install this security patch now.

Microsoft has released an emergency security patch to fix the RCE (Remote Code Execution) error on the Malware Protection Engine (MPE), allowing an attacker to execute remote code and gain control of the victim's computer.

Enabled by default, Microsoft Malware Protection Engine provides basic security features (such as scanning, detecting, deleting) for Microsoft antivirus and anti-malware software.

See also: 10 most effective antivirus software for Windows 2017

According to Microsoft, the vulnerability affects many of its security software, including Windows Defender and Microsoft Security Essentials, along with Endpoint Protection, Forefront Endpoint Protection and Exchane Server 2013 and 2016, Windows 7, Windows 8.1, Windows 10, Windows RT 8.1 and Windows Server.

Install Windows security patch now to not be hacked

The code is CVE-2017-11937, this vulnerability is actually caused by the memory failure when the Malware Protection Engine scans for fake files to detect vulnerabilities.

The vulnerability allows hackers to take control of the PC

Microsoft said the attacker placed the infected file in a location, then scanned the Malware Protection Engine for memory errors and allowed remote code execution on the LocalSystem account and took control of the target machine.

"There are many ways to place this file, such as using a website that users access," Microsoft explained. Other ways can be email, chat applications. The attacker can also "take advantage of the website to approve or store the content the user provides to upload the file to a common location, then the Malware Protection Engine scans the host server and gets an error."

Download the security patch now

Microsoft assured customers that the vulnerability was fixed before any attack. They have released security updates and recommend patching as soon as possible. Most users can receive automatic emergency patches.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937

This vulnerability was commanded by British National Network Security Center (NCSC), GCHQ's network security organization, and discovered and reported by the Department. The patch also came a few days before Microsoft released a Patch Tuesday patch for December.

See also: Microsoft released an updated patch for 25 critical security holes