Microsoft patches 0-day vulnerabilities in IE and Exchange

Getty Images | Justin Sullivan

reader comments

37 with 22 posters participating

Share this story

Microsoft’s Patch Tuesday this month had higher-than-usual stakes with fixes for a zero-day Internet Explorer vulnerability under active exploit and an Exchange Server flaw that was disclosed last month with proof-of-concept code.

The IE vulnerability, Microsoft said, allows attackers to test whether one or more files are stored on disks of vulnerable PCs. Attackers first must lure targets to a malicious site. Microsoft, without elaborating, said it has detected active exploits against the vulnerability, which is indexed as CVE-2019-0676 and affects IE version 10 or 11 running on all supported versions of Windows. The flaw was discovered by members of Google’s Project Zero vulnerability research team.

Microsoft also patched Exchange against a vulnerability that allowed remote attackers with little more than an unprivileged mailbox account to gain administrative control over the server. Dubbed PrivExchange, CVE-2019-0686 was publicly disclosed last month, along with proof-of-concept code that exploited it. In Tuesday’s advisory, Microsoft officials said they haven’t seen active exploits yet but that they were

“likely.”

Lest readers are tempted to think Microsoft is the only major software maker whose products have been actively exploited in recent weeks, Apple last week patched three iOS vulnerabilities that researchers said were being exploited as zero days in the wild. Two of those zero-days were discovered by Project Zero. Apple declined to comment.

In all, Microsoft patched more than 70 vulnerabilities, 20 of which were rated critical. Vulnerable products included IE, Edge, Windows, Office, the .NET Framework, Exchange Server, Visual Studio, the Azure IoT SDK, Microsoft Dynamics, Team Foundation Server, and Visual Studio Code. Microsoft has an overview here.

https://arstechnica.com/?p=1455587