CSO

SALTED HASH-TOP SECURITY NEWS

By Steve Ragan

About |

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Microsoft warns of new Zero-Day attack

Redmond has released a Fix It stopgap until a proper patch is available

CSO | Oct 22, 2014 2:00 AM PT

On Tuesday, Microsoft issued an advisory warning of a new Zero-Day vulnerability that impacts all supported versions of their Windows operating system except, Windows Server 2003. The software giant also confirmed targeted attacks looking to exploit this flaw.

The advisory says that attackers are using PowerPoint files, which contain a malicious Object Linking and Embedding (OLE) object, to trigger the vulnerability. OLE technology is used to share data between applications.

"The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file that contains an OLE object. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user," the advisory explained.

[How to spot a phishing email]

There are several mitigating factors including the use of User Account Control (UAC), which would warn a user once the exploit starts to trigger – asking permission to execute.

However, these warnings are often ignored, and if the attacker used Social Engineering, then the victim could be expecting the malicious file, via an email attachment or a website download.

Likewise, if the user's access levels were restricted, then a compromised host would be limited in ability.

At the same time, in corporate environments, executives and remote users are often granted administrative rights on their systems, rendering this level of mitigation obsolete – assuming that they've been restricted at all.

"All Microsoft Office file types as well as many other third-party file types could contain a malicious OLE object... In addition, compromised websites (and websites that accept or host user-provided content) could contain specially crafted content that could exploit this vulnerability," Microsoft's advisory warns.

The OLE Packager, where this latest Zero-Day was discovered by researchers at McAfee and Google, was just patched this month in MS14-060.

In response to this latest development, Microsoft has released a Fix It package for PowerPoint, and encouraged the use of EMET 5.0, to shrink the attack surface.

Furthermore, Redmond made no mention of an out-of-band patch for the Zero-Day, nor did they mention if a patch would be ready by November 11.

Steve Ragan — *Senior Staff Writer*

Insider: How a good CSO confronts inevitable bad news >