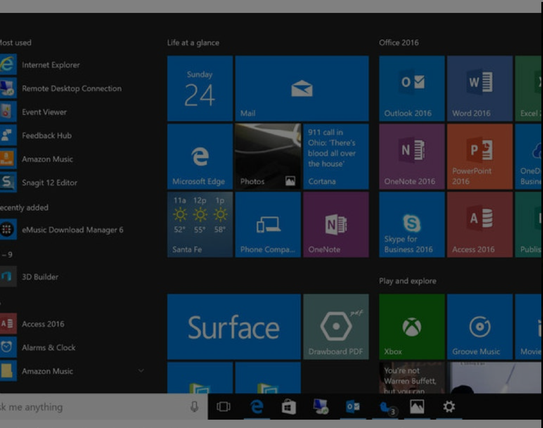
MUST READ WINDOWS 10: MICROSOFT'S POWER SLIDER PROTOTYPE LETS YOU TRADE PERFORMANCE FOR BATTERY LIFE

Windows 10 security: 'So good, it can block zero-days without being patched'

Systems running the Windows 10 Anniversary Update were shielded from two exploits even before Microsoft had issued patches for them, its researchers have found.

By Liam Tung | January 16, 2017 -- 11:54 GMT (11:54 GMT) | Topic: Security



Microsoft reckons machines running the Windows 10 Anniversary Update would not have been compromised by two zero-day flaws, unlike systems using older versions.

Image: ZDNet/Microsoft

Microsoft researchers have found that two zero-day exploits it patched against in November wouldn't have worked on systems running the Windows 10 Anniversary Update anyway.

The firm has been testing how well its latest in-built Windows 10 and Edge exploit-mitigation features such as AppContainer sandboxing and stronger validation, which shipped with the Anniversary Update (https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf) in August, can block commonly used techniques.

Microsoft's Windows Defender security team tested the Anniversary Update against CVE-2016-7255, a zero-day flaw used by the Fancy Bear hackers (http://www.zdnet.com/article/russian-hacking-group-sharpens-skills/) targeting US organizations in October, and CVE-2016-7256, which was used against South Korean targets. Both kernel-level exploits resulted in elevation of privileges and were patched in November.

While systems running older versions of Windows would have been compromised, systems on the Anniversary Update would have been protected, according to Microsoft's analysis.

"We saw how exploit-mitigation techniques in Windows 10 Anniversary Update, which was released months before these zero-day attacks, managed to neutralize not only the specific exploits but also their exploit methods," Microsoft's Windows Defender ATP Research Team write (https://blogs.technet.microsoft.com/mmpc/2017/01/13/hardening-windows-10-with-zero-day-exploit-mitigations/).

"As a result, these mitigation techniques are significantly reducing attack surfaces that would have been available to future zero-day exploits."

As they noted, fixing a single vulnerability helps neutralize a specific bug. However, boosting exploit mitigation can take out attack techniques used across multiple exploits.

"Such mitigation techniques can break exploit methods, providing a medium-term tactical benefit, or close entire classes of vulnerabilities for long-term strategic impact," the Defender team wrote.

SEE ALL OF ED BOTT'S WINDOWS 10 TIPS

Solve network problems with a one-click reset (http://www.zdnet.com/article/windows-10-tip-solve-network-problems-with-a-one-click-reset/)

Shut down OneDrive completely (http://www.zdnet.com/article/windows-10-tip-shut-down-onedrive-completely/)

Squeeze hours of extra life from your laptop battery (http://www.zdnet.com/article/windows-10-tip-squeeze-hours-of-extra-life-from-your-laptop-battery/)

Find your PC's original product key (http://www.zdnet.com/article/windows-10-tip-find-your-pcs-original-product-key/)

Stay organized using virtual desktops (http://www.zdnet.com/article/windows-10-tip-stay-organized-using-virtual-desktops/)

Change UEFI firmware settings or start in Safe Mode (http://www.zdnet.com/article/windows-

desktops (http://www.zdnet.com/article/windows-10-tip-stay-organized-using-virtual-desktops/)

For example, CVE-2016-7255, a Win32k exploit used in conjunction with a Flash Player zero-day, abused the Windows tagWND.strName. The attackers obtained read-write (RW) primitives by corrupting the tagWND.strName kernel structure, explained the team, noting that the exact same method was used by advanced malware discovered in 2015 called Duqu 2.0 (https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/).

The Windows 10 Anniversary Update prevents abuse of tagWND.strName through additional validation, ensuring they can't be used for RW primitives.

"In our tests on Anniversary Update, exploits using this method to create an RW primitive in the kernel are ineffective. These exploits instead cause exceptions and subsequent blue-screen errors," write the team.

Meanwhile, Microsoft's security team found that the exploit for CVE-2016-7256 was neutralized by running font-parsing in the AppContainer sandbox rather than the Windows kernel.

"Windows 10 Anniversary Update also includes additional validation for font-file parsing. In our tests, the specific exploit code for CVE-2016-7256 simply fails these checks and is unable to reach vulnerable code."

Microsoft plans to reveal more exploit-mitigation features in the forthcoming Windows 10 Creators Update, which is due in the spring (http://www.zdnet.com/article/windows-10-creators-update-whats-on-tap-for-spring-2017-for-business-users/).

Microsoft has justified dropping support for its standalone (http://www.zdnet.com/article/microsoft-delays-enhanced-mitigation-experience-toolkit-support-cut-off-to-july-2018/) exploit-mitigation toolset EMET because these security features are being built in to Windows 10.

EMET support ends on July 13, 2018, so if Windows 7 users want the additional protection once provided by EMET, they'll have to upgrade to Windows 10 before Windows 7 extended support expires in 2020.

READ MORE ABOUT WINDOWS 10

- New Windows 10 build incoming: Microsoft nixes annoying productivity obstacles (http://www.zdnet.com/article/new-windows-10-build-incoming-microsoft-nixes-annoying-productivity-obstacles)
- Microsoft's 2016: Windows 10 foibles and futures are the big stories (http://www.zdnet.com/article/microsofts-2016-windows-10-foibles-and-futures-are-the-big-stories)
- Windows 10 tip: Find and decode secret version details (http://www.zdnet.com/article/windows-10-tip-decode-detailed-version-information)

JOIN DISCUSSION